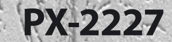



DEU

# Outdoor Router

## und Access Point 14 dBi

Bedienungsanleitung

7Links™

# Outdoor Router
## und Access Point 14 dBi

# INHALTSVERZEICHNIS

## EINLEITUNG



## INSTALLATIONSANLEITUNG FÜR EINSTEIGER







## DETAILLIERTE ERLÄUTERUNGEN ZUR KONFIGURATION



## ANHANG

# EINLEITUNG

# IHR NEUER WLAN-ROUTER

**Sehr geehrte Kunden,**

vielen Dank für den Kauf dieses Outdoor-WLAN-Routers.
Mit dieser innovativen Lösung aus dem Hause 7Links haben Sie nun auch als Privatanwender die Möglichkeit Ihr WLAN-Netz auch nach draußen zu erweitern und so mit Ihrem Notebook Zugriff auf das Internet zu haben, während Sie sich gemütlich im Liegestuhl sonnen.
Aber auch im professionellen Bereich können Sie mit diesem Router teure Verkabelungsmaßnahmen vermeiden und Bereiche, die sonst nicht an das Firmennetz angeschlossen werden könnten, mit einem Netzzugang versorgen.
Bitte lesen Sie die Bedienungsanleitung und befolgen Sie die Hinweise und Tipps, damit Sie diesen WLAN-Router optimal nutzen können.

# HINWEISE ZUR NUTZUNG DIESER BEDIENUNGSANLEITUNG

Um diese Bedienungsanleitung möglichst effektiv nutzen zu können, ist es notwendig, vorab einige Begriffe und Symbole zu erläutern, die Ihnen im Verlauf dieser Anleitung begegnen werden.

**Verwendete Symbole**

| | |
|---|---|
| | Dieses Symbol steht für mögliche Gefahren und wichtige Informationen im Umgang mit diesem Produkt. Es wird immer dann verwendet, wenn der Anwender eindringlich auf etwas hingewiesen werden soll. |
| | Dieses Symbol steht für nützliche Hinweise und Informationen, die im Umgang mit dem Produkt helfen sollen „Klippen zu umschiffen" und „Hürden zu nehmen". |
| | Dieses Symbol wird für beispielhafte Anwendungen und Erläuterungen verwendet, die oft komplexe Vorgehensweisen veranschaulichen und begreiflich machen sollen. |
| | Dieses Symbol wird oftmals hinter Fachbegriffen zu finden sein, zu denen weitere Erläuterungen im Glossar zu finden sind. Das Glossar soll dabei helfen, diese Fachbegriffe für den Laien verständlich zu machen und in einen Zusammenhang zu rücken. |

### Verwendete Textmittel

| | |
|---|---|
| GROSSBUCHSTABEN | Großbuchstaben werden immer dann verwendet, wenn es gilt Tasten, Anschluss- oder andere Produkt-Beschriftungen kenntlich zu machen. |
| **Fettschrift** | Fettschrift wird immer dann eingesetzt, wenn Menüpunkte oder genau so bezeichnete Ausdrücke in der Software des Produktes verwendet werden. |
| • Aufzählungen<br>• | Aufzählungen werden immer dann verwendet, wenn der Anwender eine bestimmte Reihenfolge von Schritten befolgen soll, oder die Merkmale des Produktes beziffert werden sollen. |
| 1. Unterpunkte<br>2. | Unterpunkte werden immer dann verwendet, wenn mehrere Informationen aufgelistet werden. Sie dienen hauptsächlich zum besseren kenntlich Machen der einzelnen Informationen. |
| < Platzhalter > | Im zweiten Teil des Handbuches werden Platzhalter verwendet. Diese Platzhalter werden in < und > Zeichen eingegrenzt.<br>• <text> bedeutet hierbei die Möglichkeit freie Eingaben zu machen (oftmals IP-Adressen).<br>• <parameter> bedeutet die Möglichkeit mehrere benötigte Daten einzugeben.<br>• <datei> wird verwendet, wenn ein Dateiname erforderlich ist.<br>• <hexcode> bezeichnet eine Eingabe in Hexadezimalen Ziffern. |





### Gliederung

Diese Anleitung ist untergliedert in vier grundlegende Bestandteile:

| | |
|---|---|
| **Einleitung** | Erläuterungen zur Nutzung dieser Anleitung, Wichtige Hinweise zur Sicherheit im Umgang mit dem Produkt, Übersicht über das Produkt |
| **Installationsanleitung für Einsteiger** | Detaillierte Anleitung zur Installation und Inbetriebnahme des Routers in einem bestehenden WLAN-Netzwerk, oder als allein stehender Router. Anleitung zur Konfiguration von grundlegenden Sicherheitsmaßnahmen. |
| **Detaillierte Erläuterungen zur Konfiguration** | Dieser Teil der Anleitung richtet sich insbesondere an fortgeschrittene Anwender und Profis. Hier finden sich genaue Informationen zu den einzelnen Konfigurationsmöglichkeiten und Anwendungsbeispiele für den Einsatz des Routers in größeren Netzwerken und Betrieben. |
| **Anhang** | Troubleshooting (Problemlösungen), Glossar, Technische Daten, Konformitätserklärung, Index |

# SICHERHEITSHINWEISE & GEWÄHRLEISTUNG

- Diese Bedienungsanleitung dient dazu, Sie mit der Funktionsweise dieses Produktes vertraut zu machen. Bewahren Sie diese Anleitung daher stets gut auf, damit Sie jederzeit darauf zugreifen können.
- Sie erhalten bei Kauf dieses Produktes zwei Jahre Gewährleistung auf Defekt bei sachgemäßem Gebrauch. Bitte beachten Sie auch die allgemeinen Geschäftsbedingungen!
- Bitte verwenden Sie das Produkt nur in seiner bestimmungsgemäßen Art und Weise. Eine anderweitige Verwendung führt eventuell zu Beschädigungen am Produkt oder in der Umgebung des Produktes.
- Ein Umbauen oder Verändern des Produktes beeinträchtigt die Produktsicherheit. Achtung Verletzungsgefahr!
- Führen Sie Reparaturen nie selber aus!
- Behandeln Sie das Produkt sorgfältig. Es kann durch Stöße, Schläge oder Fall aus bereits geringer Höhe beschädigt werden.
- Halten Sie das Produkt fern von Feuchtigkeit und extremer Hitze.
- Tauchen Sie das Produkt niemals in Wasser oder andere Flüssigkeiten.
- Montieren Sie das Produkt nicht an Orten, die extremen Umweltbedingungen ausgesetzt sind (pralle Sonne, Wetterkanten), um Beeinträchtigungen der Funktionalität zu vermeiden.
- Verwenden Sie nur die mitgelieferten oder andere geeignete Montagemittel, um das Produkt sicher zu befestigen.
- Berühren Sie die Elektronik nicht im Betrieb! Es besteht die Gefahr eines Stromschlags!
- Fassen Sie nicht auf die Platine der Elektronik, das Produkt kann dadurch beschädigt werden.
- Schließen Sie das Produkt nicht an extrem gespannte Kabel an. Die Anschlüsse können sonst beschädigt werden.
- Verlegen Sie Kabel möglichst unzugänglich in Kabelkanälen, um Beschädigungen und „Stolperfallen“ zu vermeiden.
- Verwenden Sie Funkprodukte niemals in direkter Nähe von Personen mit elektronischen Herzschrittmachern!
- Verwenden Sie zur Stromversorgung ausschließlich das mitgelieferte Netzteil!

***ACHTUNG***
***Es wird keine Haftung für Folgeschäden übernommen.***
***Technische Änderungen und Irrtümer vorbehalten!***

# KONFORMITÄTSERKLÄRUNG

Hiermit erklärt Pearl Agency, dass sich dieses Produkt PX-2227-675 in Übereinstimmung mit den grundlegenden Anforderungen der Richtlinie 1999/5/EG befindet.

Pearl Agency
Pearl-Str. 1-3
79426 Buggingen
Deutschland
30.11.2009

Die ausführliche Konformitätserklärung finden Sie unter www.pearl.de.

# PRODUKTDETAILS

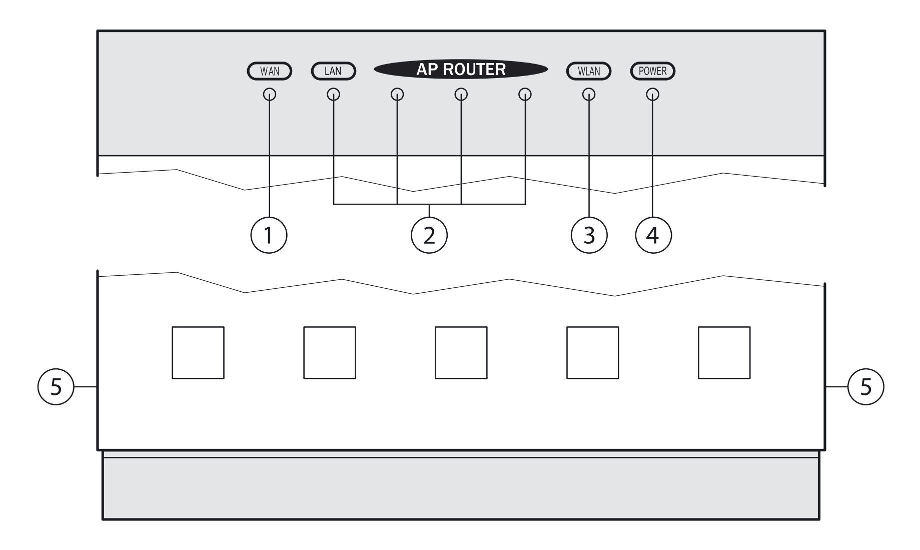


**Lieferumfang**
- WLAN-Router
- Netzteil (12 V / 1 A)
- Kabelklemme
- 2 Rohrklemmen
- 2 Nägel
- Bedienungsanleitung

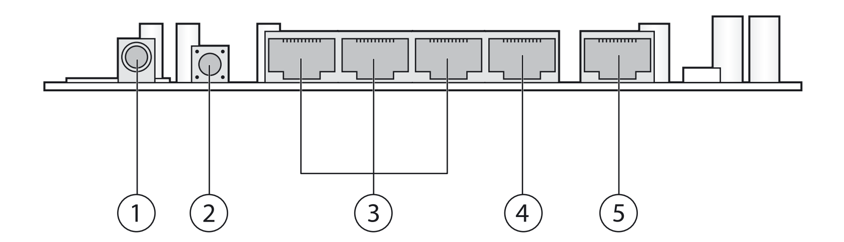
**Produktinformationen**
Der WLAN-Router wurde speziell für den Outdoor-Bereich entwickelt und bietet neben reinen Routingaufgaben auch die Möglichkeit als Bridge oder als WLAN-Repeater zu fungieren.
Dadurch lässt sich dieses Produkt äußerst vielseitig einsetzen und bietet sowohl dem Heimanwender, als auch professionellen Nutzern eine Vielzahl an Anwendungsgebieten.
Komplettiert werden die Standard-Funktionen des Routers durch die Unterstützung einer virtuellen DMZ, DDNS, DoS-Response, QoS und die Möglichkeit der Ansteuerung eines Watchdog-Rechners.
Damit lassen sich sowohl private Netzwerke, als auch Netzwerke kleinerer und mittlerer Betriebe optimal gegen Einflüsse von außen abschirmen.
Hierzu stehen ebenfalls die, zum heutigen Sicherheitsstandard gehörenden, Verschlüsselungsvarianten WPA und WPA2 zur Verfügung – und auch RADIUS-Server werden unterstützt.
Mit den 802.11b/g Standards erreichen Sie Datendurchsatzraten bis zu 54 MBit/s. Die 14dBi-Panel-Antenne ermöglicht hierbei einen verlustarmen Datentransfer über weite Strecken. Unter normalen Umweltbedingungen werden Entfernungen von 300 m problemlos überbrückt, im Idealfall erreichen Sie sogar weitaus größere Entfernungen (bis etwa 500 m).

**Betriebs-LEDs**
1. WAN-LED: zeigt den Status der Hauptverbindung an.
2. LAN-LEDs: zeigen den Status der Nebenverbindungen an.
3. WLAN-LED: zeigt den Status des WLANs an.
4. POWER-LED: zeigt den Betriebszustand an.

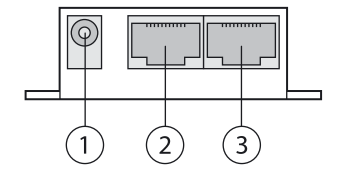
5. Gehäuserasten: hier öffnen Sie das Gehäuse.




**Router-Anschlüsse**
1. Antennenanschluss
2. Reset-Taste
3. LAN2-4 Ports (ohne POE ◪)
4. LAN1-Port (mit POE ◪)
5. WAN-Port (mit POE ◪)



**POE-Box**
1. Strom-Anschluss
2. POE-Port
3. LAN-Port








# VORBEREITUNG UND MONTAGE

*HINWEIS:*
*Viele der Fachbegriffe werden im Anhang „Basiswissen Netzwerke“ erläutert (S.88 ff). Sollten dennoch Fragen bezüglich der Installation bestehen, können Sie sich gerne an unsere Service-Hotline wenden.*

**Benötigtes Zubehör**
Um den WLAN-Router zu montieren und in Ihr Netzwerk integrieren zu können benötigen Sie folgendes Zubehör:

- 2 Netzwerkkabel (CAT5- oder CAT6-Patchkabel) in ausreichender Länge
- Montagezubehör, sofern Sie den Router nicht an einer Wand oder einem Rohr (max. 1,25") befestigen wollen.
- Werkzeug zur Montage des Routers.

**Produktempfehlungen**
Zusätzlich zu den unbedingt notwendigen Zubehörteilen werden für die Erweiterung Ihres Netzwerkes weitere Artikel empfohlen. Die folgenden Produkte sind im Internet unter www.pearl.de erhältlich:

| | |
|---|---|
| PE-8419 | Netzwerkkabel Twisted Pair 2 x RJ45 Stecker-Stecker 20 m |
| PE-219 | Netzwerkkabel Twisted Pair 2 x RJ45 Stecker-Stecker 10 m |
| PE-218 | Netzwerkkabel Twisted Pair 2 x RJ45 Stecker-Stecker 5 m |
| PE-217 | Netzwerkkabel Twisted Pair 2 x RJ45 Stecker-Stecker 3 m |
| PE-5586 | ConnecTec 10/100MBit Netzwerk-Switch 5-Port USB mit blauen LEDs |
| PX-6516 | TP-LINK 54Mbit WLAN-USB-Dongle „TL-WN321G“ USB2.0 (802.11g/b) |
| PE-4454 | revolt Profi-Steckdosenleiste mit Netzwerkschutz |

## Vorbereitung

*HINWEIS:*
*Sollten Sie sich bei den folgenden Fragen nicht sicher sein, empfehlen wir Ihnen, sich an Fachpersonal zu wenden. Eine Fehlkonfiguration des Routers kann unter bestimmten Umständen Ihr Netzwerk beträchtlich in der Funktion stören.*

Um eine reibungslose Installation des Routers gewährleisten zu können, sollten Sie folgende Daten im Vorfeld recherchieren und bereithalten:

1. Die Zugangsdaten Ihres Serviceproviders (Internet-Anbieters)
2. Die IP-Adresse ◪ des Gateway-Routers ◪, sofern Sie den WLAN-Router nicht als einzigen Router im Netzwerk betreiben wollen.
3. Wird in Ihrem Netzwerk bereits ein DHCP-Server ◪ verwendet? Wenn ja – welche Adressräume deckt dieser ab?
4. Welche Protokolle◪ werden für verschiedene Anwendungen verwendet und benötigt (etwa uPnP ◪)?

Ferner sollten Sie folgendes im Vorfeld beachten:

- Bei der Erstinstallation sollte der Router direkt über Kabel mit einem Computer verbunden werden.
- Beseitigen Sie eventuelle Störquellen im Funktionsbereich des WLAN-Routers. Hierzu gehören Funktelefone, Funküberwachungskameras und andere Geräte, die mit dem 2,4 GHz Band funktionieren.
- Bringen Sie die POE-Box ◪ im Innern an und sichern Sie die Stromversorgung möglichst mit einem Überspannungsschutz.
- Verwenden Sie zwischen POE-Box und Router kein Kabel, das länger als 25 m ist – bei ungünstigen Verhältnissen kann es sonst zu einem Spannungsabfall kommen und der Router wird nicht mehr ausreichend mit Strom versorgt.
- Schalten Sie zur Einbindung des Routers in ein bestehendes Netzwerk alle Firewalls ◪, Virenscanner, MAC-Adressenfilter ◪ und Verschlüsselungen ◪ bei Ihrem bereits vorhandenen Router aus.
- Notieren Sie sich die SSID ◪ Ihres bestehenden WLAN-Netzwerks.

*HINWEIS:*
*Im Anhang (S.87) finden Sie eine Checkliste die Ihnen als Stütze dienen soll und in die Sie die entsprechenden Werte eintragen können. Trennen Sie die Checkliste einfach mit einer Schere an der Schnittmarke heraus, um sich lästiges Umblättern zu ersparen.*

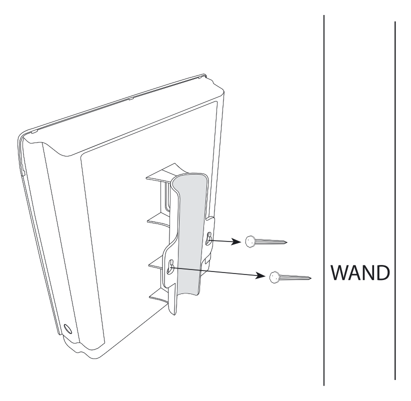




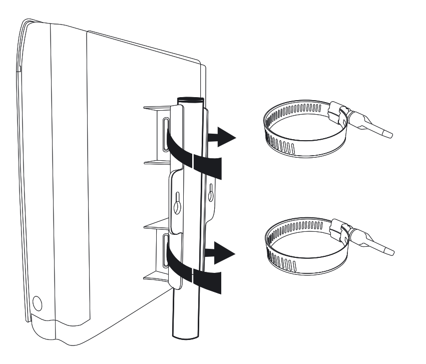
## Montage

***ACHTUNG:***
***Bringen Sie den Router nur an Stellen an, die nicht direkt der Witterung und direkter Sonneneinstrahlung ausgesetzt sind.***

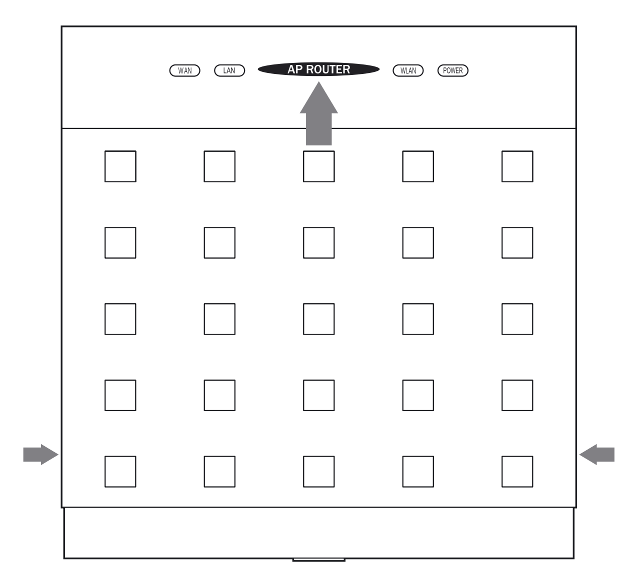
Bringen Sie den Router an einer geeigneten Stelle im Freien an.
Zur Wandmontage befestigen Sie entweder die beiden mitgelieferten Nägel oder verdübelte Schrauben im Abstand von 6 cm an der gewünschten Position. Haken Sie danach den Router in die vorgefertigten Aufhängungen ein.



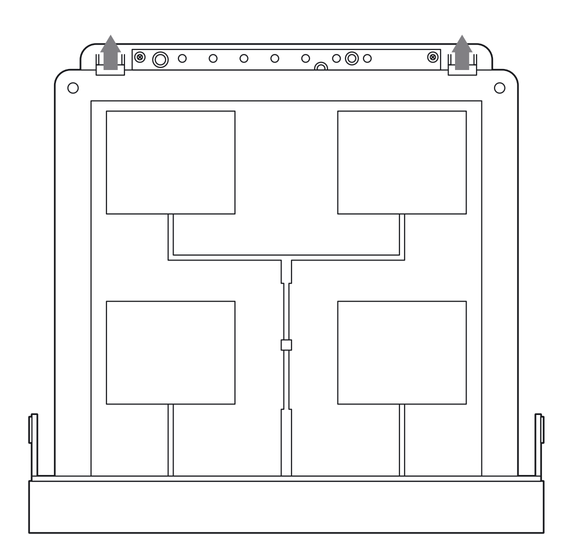

Zur Rohrmontage führen Sie die beiden Rohrschellen durch die Aufhängungs-schlitze an der Rückseite des Routers. Legen Sie nun den Router an das Rohr an und drehen Sie die Rohrschellen in der gewünschten Höhe fest.



Drücken Sie nun die beiden Gehäuserasten nach innen und ziehen Sie das Gehäuse des Routers nach oben hin ab.



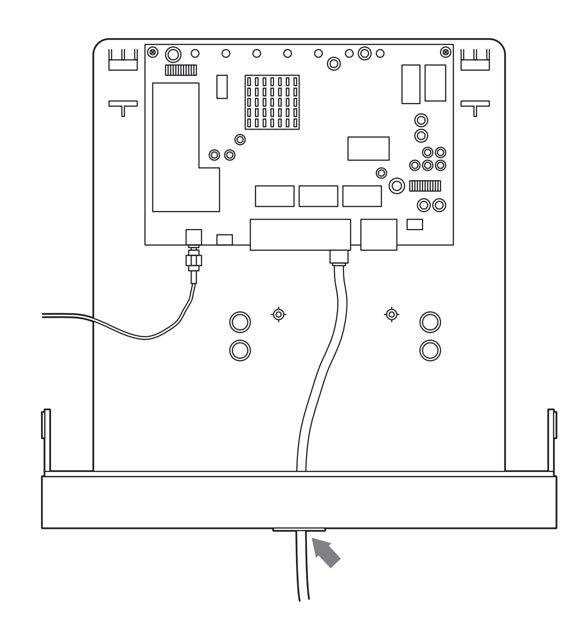

Nehmen Sie nun die Antennenplatte ab, indem Sie die oberen Halteklammern nach oben drücken und die Platte aus den unteren Halteschienen heben.







Führen Sie nun ein Netzwerkkabel durch die Kabelführung und rasten Sie diese in das Zuführungsloch an der Unterseite des Gehäuses ein.



**Verkabelung**
Verbinden Sie den Stecker des Netzwerkskabels mit dem WAN-Port des Routers.
Schieben Sie nun die Antennenplatte wieder in die dafür vorgesehenen Halteschienen und rasten sie in die Halteclips ein.
Verschließen Sie dann das Gehäuse.
Verlegen Sie das Netzwerkkabel möglichst unzugänglich für Dritte ins Innere des Hauses. Achten Sie unbedingt darauf, unterhalb des Routers eine Abtropfschlaufe einzurichten.

*HINWEIS:*
*Beim Verlegen des Kabels sollten Sie darauf achten, das Kabel nicht einzuklemmen oder anderweitig zu beschädigen. Ziehen Sie gegebenenfalls Fachpersonal zu Rate.*

Schließen Sie nun das Gehäuse des Routers wieder.

**Die POE-Box**
Montieren Sie die POE-Box an einer geeigneten Stelle im Inneren des Hauses.

*HINWEIS:*
*Die Länge des Kabels des Netzteils beträgt etwa 180 cm, daher sollte die POE-Box nicht weiter entfernt als 160 cm von einer Steckdose angebracht werden.*

Verbinden Sie nun zuerst das Netzwerkkabel des Routers mit dem POE-Port.
Anschließend verbinden Sie das Netzwerkkabel zum Computer mit dem LAN-Port der POE-Box.
Zuletzt verbinden Sie das Netzteil mit der Stromversorgung und der POE-Box.





# INSTALLATIONSANLEITUNG FÜR EINSTEIGER

# DIE INSTALLATION



**Den Computer vorbereiten**
Im Auslieferungszustand ist der DHCP-Server des Routers aktiviert.
Daher sollte der Konfigurationscomputer ebenfalls auf DHCP-Zuweisung umgestellt werden, sofern dies nicht bereits der Fall ist.

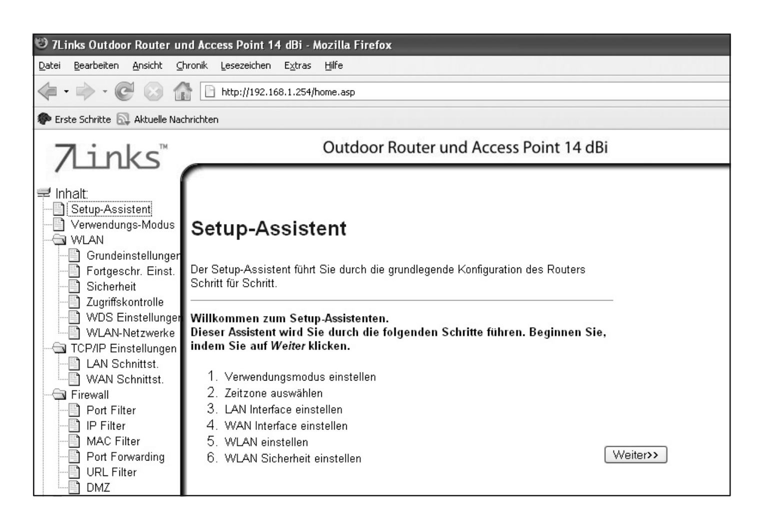
- **Vorgehensweise unter Windows 2000 und Windows XP**
  1. Klicken Sie auf den Start-Button.
  2. Klicken Sie auf **Systemsteuerung**.
  3. Wählen Sie **Netzwerkverbindungen**.
  4. Doppelklicken Sie die aktive LAN-Verbindung (unter **Status** steht **Verbindung hergestellt**).
  5. Klicken Sie auf **Eigenschaften**.
  6. Markieren Sie im Auswahlfenster **Internetprotokoll (TCP/IP)** und klicken Sie auf **Eigenschaften**.
  7. Wählen Sie **IP-Adresse automatisch beziehen** und **DNS-Serveradresse automatisch beziehen** aus und bestätigen Sie mit **OK**, um die Änderungen zu speichern.

- **Vorgehensweise unter Windows Vista und Windows 7**
  1. Klicken Sie auf den Start-Button.
  2. Klicken Sie auf **Systemsteuerung**.
  3. Wählen Sie **Netzwerk- und Freigabecenter**.
  4. Klicken Sie die hinter der aktiven LAN-Verbindung auf **Status anzeigen**.
  5. Klicken Sie auf **Eigenschaften**.
  6. Markieren Sie im Auswahlfenster **Internetprotokoll Version 4 (TCP/IPv4)** und klicken Sie auf **Eigenschaften**.
  7. Wählen Sie **IP-Adresse automatisch beziehen** und **DNS-Serveradresse automatisch beziehen** aus und bestätigen Sie mit **OK**, um die Änderungen zu speichern.

**Der erste Zugriff auf den Router**

*HINWEIS:*
*Um die Konfigurationsseite des Routers korrekt darzustellen, muss in Ihrem Browser die Darstellung von JavaScript erlaubt sein.*
*Ziehen Sie gegebenenfalls die Hilfefunktion Ihres Browsers zu Rate.*

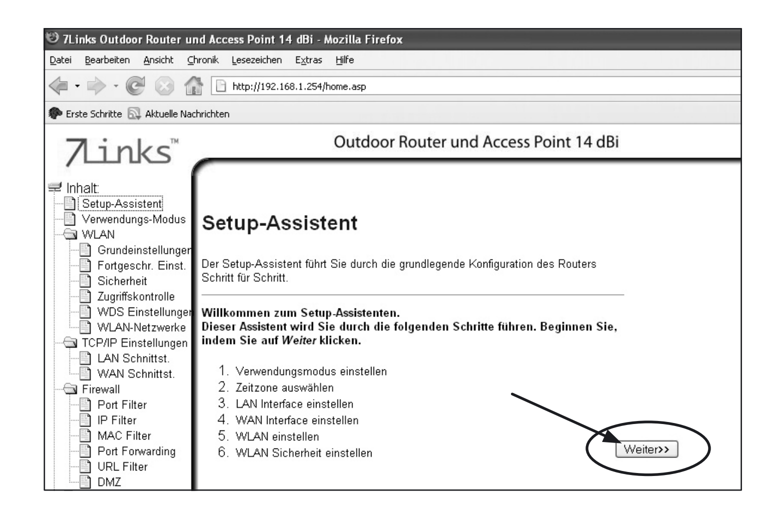
Starten Sie auf dem Computer einen Browser (wie etwa den **Internet Explorer, Firefox,** oder ähnliche).
Geben Sie in der Adresszeile des Browsers die IP-Adresse des Routers ein, um zum Konfigurationsbildschirm zu gelangen. Bei der ersten Installation ist die IP-Adresse des Routers **192.168.1.254**. Diese Adresse können Sie im Verlauf der Erstinstallation ändern.
Nachdem Sie die Adresse eingegeben haben, zeigt Ihr Browser die Konfigurationsseite des Routers an.



## Die Konfiguration als Zweitrouter

*ACHTUNG:*
***In diesem Kapitel wird davon ausgegangen, dass Sie den Router als Zweitrouter verwenden und nicht direkt eine Verbindung zum Internet mit diesem Router herstellen. Sollten Sie den Router jedoch als einzigen Router im Netzwerk verwenden, lesen Sie bitte im Kapitel* Die Konfiguration als einzelner Router *auf S.31 weiter.***

- **Vorkonfiguration des Routers**
  Um den Router für den Einsatz in Ihrem bestehenden Netzwerk vorzubereiten, verwenden Sie den **Setup Assistenten**. Dieser Assistent erlaubt eine schnelle und unkomplizierte Einbindung.
  Klicken im Eröffnungsbildschirm einfach auf **Weiter,** um den Assistenten zu starten.

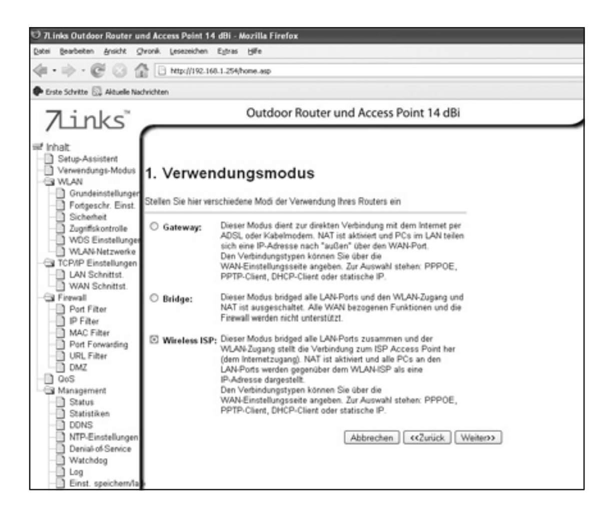



Wählen Sie im nächsten Bildschirm, dass Sie den Router als **Wireless ISP** verwenden wollen. Bestätigen Sie die Auswahl mit **Weiter.**

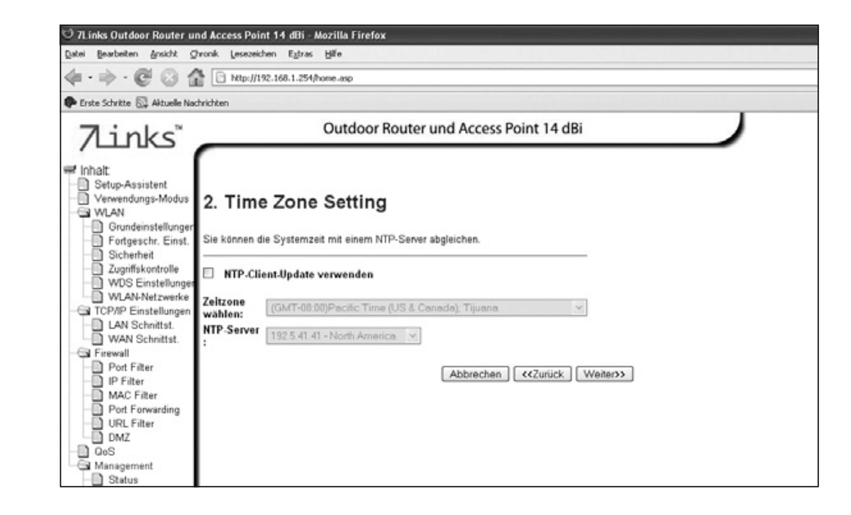
*HINWEIS:*
***Wireless ISP** legt fest, dass Sie sich mit einem zweiten WLAN-Router verbinden wollen, welcher den Zugang zum Internet darstellt.*



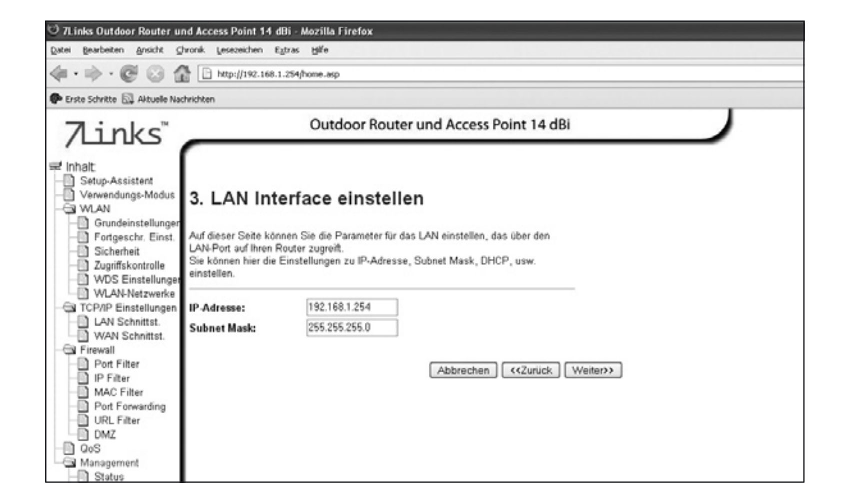





Im nächsten Schritt können Sie einen Zeitzonenserver angeben, mit dem die Systemzeit synchronisiert werden kann. Dies ist jedoch nicht unbedingt notwendig!
Bestätigen Sie daher den Assistenten mit **Weiter.**



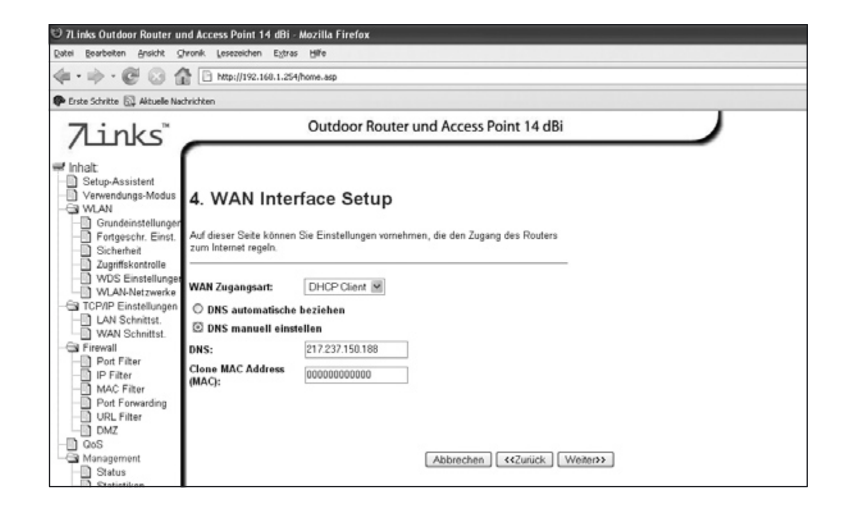
Dieser Schritt ist für die Festlegung einer IP-Adresse der LAN-Verbindung notwendig. Der Standardwert für die IP-Adresse ist **192.168.1.254**. Sie können diesen Wert unverändert lassen oder diesen – was empfohlen wird – auf einen anderen Wert einstellen.
Verwenden Sie z.B. **192.168.1.2**. Üblicherweise werden Router mit einem voreingestellten Adressbereich von 192.168.1.1 – 192.168.1.254 ausgeliefert. Somit ist eine Platzierung im gleichen Adressbereich von Vorteil.
Klicken Sie anschließend auf **Weiter**, um mit der Konfiguration fortzufahren.



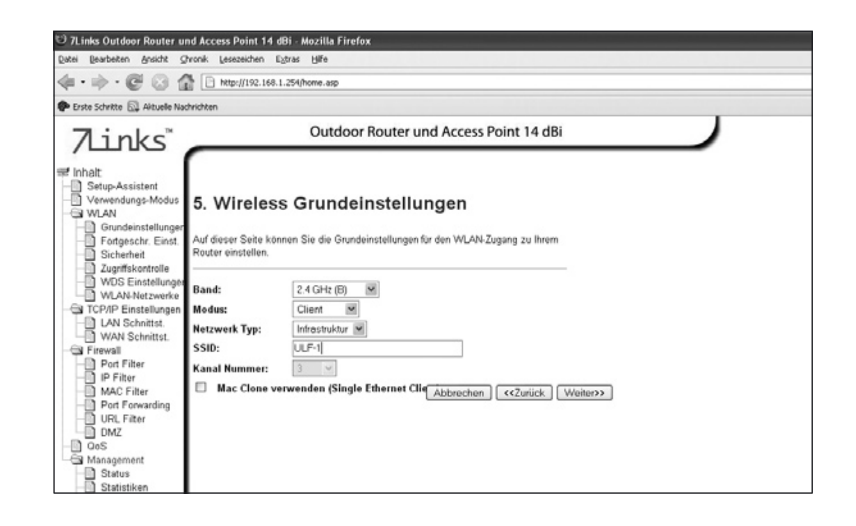

Bei der WAN-Konfiguration geben Sie an, ob Sie sich direkt mit dem Internet verbinden, oder ob die Verbindung über einen zweiten Router erfolgen soll. In diesem Bereich der Anleitung wird davon ausgegangen, dass Sie bereits einen WLAN-Router in Betrieb haben. Stellen Sie daher die WAN-Zugangsart **DHCP Client** ein. Ebenfalls muss die Option **DNS manuell einstellen** ausgewählt sein. Tragen Sie im rechten Feld neben **DNS** die DNS-Adresse Ihres Internetanbieters ein.
Bestätigen Sie mit Klick auf **Weiter.**





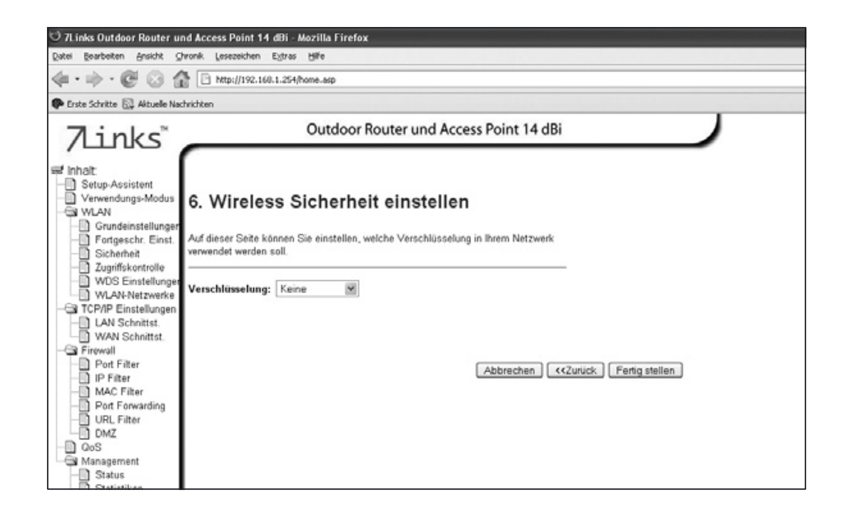



Im nächsten Schritt werden Sie aufgefordert, Daten zum bestehenden Netzwerk und der Betriebsart einzustellen.
Verwenden Sie hier als Band die Option **2.4 GHz (B+G)**, den Modus **Client**, als Netzwerktyp **Infrastruktur** und als SSID die Bezeichnung Ihres bestehenden WLAN-Netzwerks (z.B. **ULF-1**).



Der letzte Konfigurationsschritt dient zur Festlegung der Netzwerksicherheit. Stellen Sie hier als Verschlüsselung **keine** ein. Dies verhindert, dass es bei der ersten Verbindung Ihres neuen Routers in das bestehende WLAN-Netzwerk zu unvorhersehbaren Problemen kommt. Klicken Sie abschließend auf **Fertig stellen**, um die Erstkonfiguration abzuschließen.

*HINWEIS:*
*Nachdem Ihr Router in das bestehende Netzwerk eingebunden wurde, wird empfohlen im Menüpunkt* ***Sicherheit*** *(Unterpunkt von* ***WLAN****) eine sichere Verschlüsselungsmethode festzulegen!*



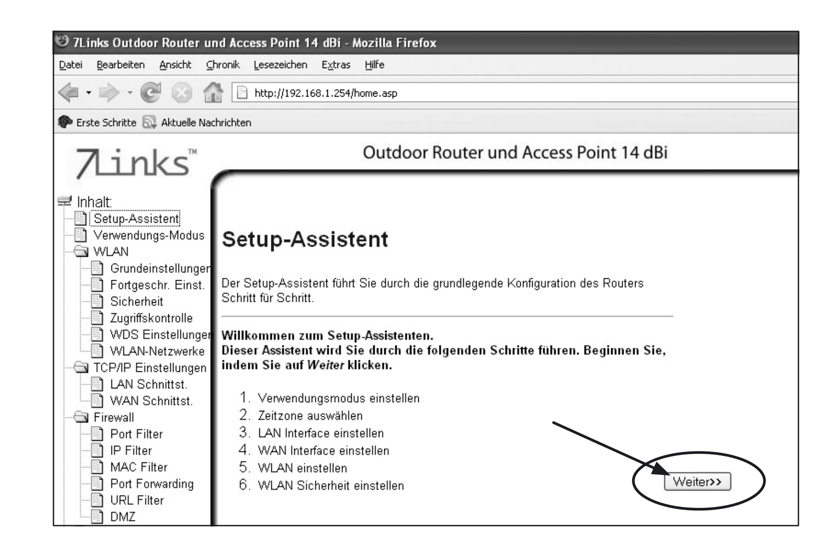




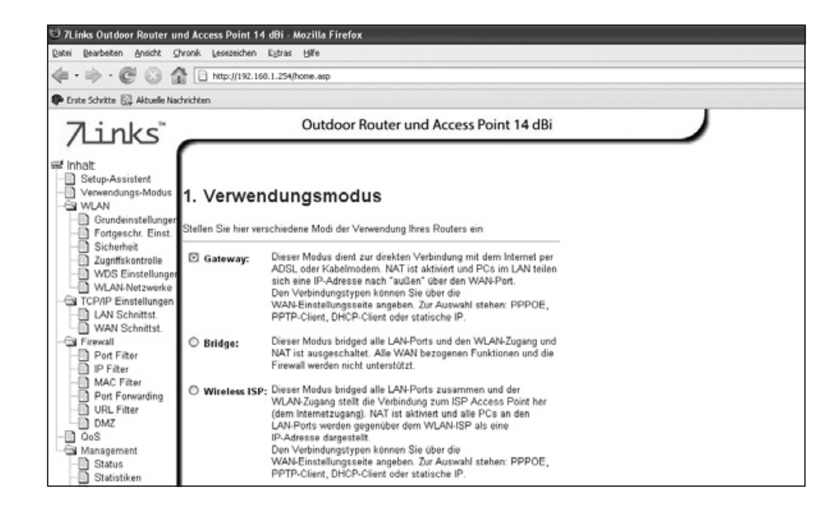

## Die Konfiguration als einzelner Router

***ACHTUNG:***
***In diesem Kapitel wird davon ausgegangen, dass Sie den Router als alleinigen Router verwenden und direkt eine Verbindung zum Internet mit diesem Router herstellen. Sollten Sie den Router jedoch als zweiten Router im Netzwerk verwenden, lesen Sie bitte im Kapitel*** **Die Konfiguration als Zweitrouter** ***auf S.26 weiter.***

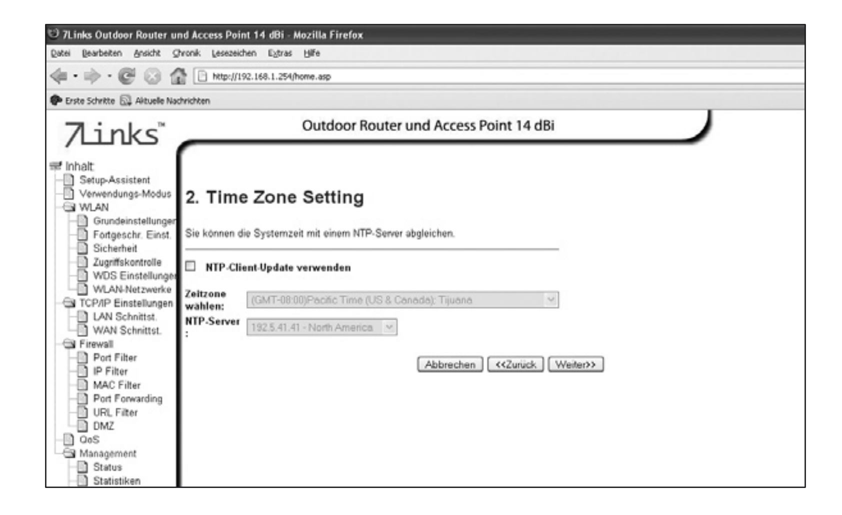
- **Vorkonfiguration des Routers**
  Um den Router für den Einsatz in Ihrem Netzwerk vorzubereiten, verwenden Sie den **Setup-Assistenten**. Dieser Assistent erlaubt eine schnelle und unkomplizierte Einbindung. Klicken im Eröffnungsbildschirm einfach auf **Weiter,** um den Assistenten zu starten.



Zur direkten Verbindung mit dem Internet muss hier die Option **Gateway** ausgewählt werden.



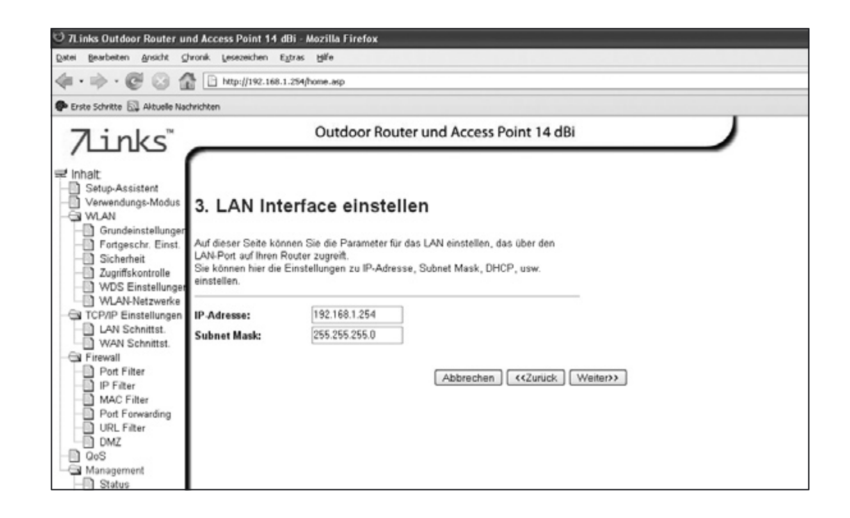

Im nächsten Schritt können Sie einen Zeitzonenserver angeben, mit dem die Systemzeit synchronisiert werden kann. Dies ist jedoch nicht unbedingt notwendig.
Bestätigen Sie daher den Assistenten mit **Weiter.**



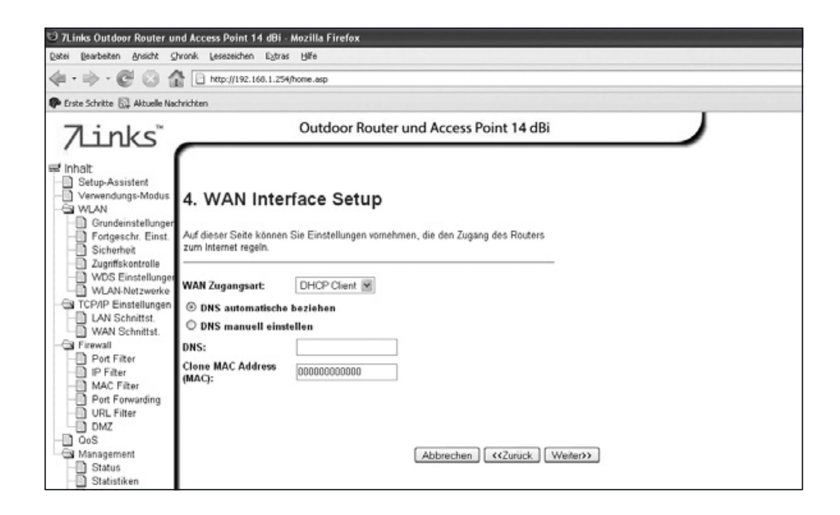





Dieser Schritt ist für die Festlegung einer IP-Adresse der LAN-Verbindung notwendig. Der Standardwert für die IP-Adresse ist **192.168.1.254**. Sie können diesen Wert unverändert lassen oder diesen – was empfohlen wird – auf einen anderen Wert einstellen. Verwenden Sie z.B. 192.168.1.1. Üblicherweise werden Router mit einem voreingestellten Adressbereich von 192.168.1.1 – 192.168.1.254 ausgeliefert. Somit ist eine Platzierung in diesem Adressbereich von Vorteil, da sich die Anleitungen zu Netzwerkgeräten oft an diese Werte anlehnen. Klicken Sie anschließend auf **Weiter,** um mit der Konfiguration fortzufahren.



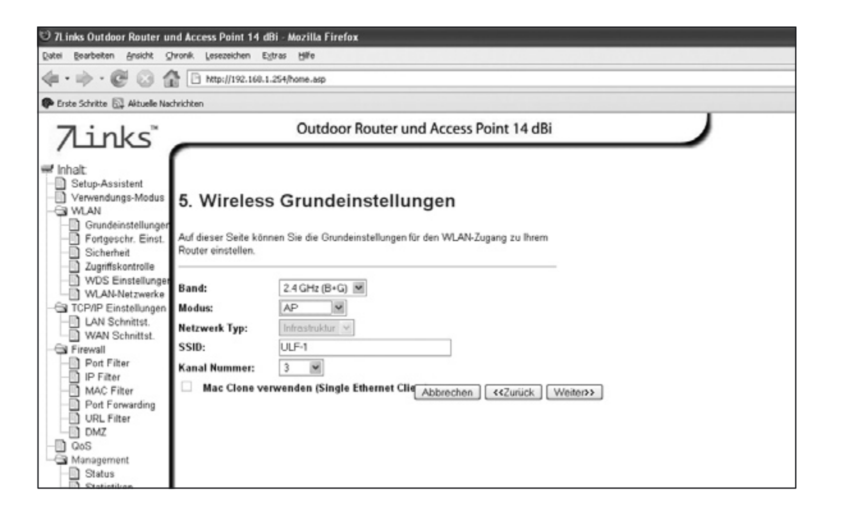
Bei der WAN-Konfiguration geben Sie an, ob Sie sich direkt mit dem Internet verbinden, oder ob die Verbindung über einen zweiten Router erfolgen soll. In diesem Bereich der Anleitung wird davon ausgegangen, dass Sie den WLAN-Router direkt mit dem Internet über einen DSL-Anschluss oder Kabelmodem verbinden.
Stellen Sie daher die WAN-Zugangsart **DHCP Client** ein. Ebenfalls muss die Option **DNS automatisch beziehen** ausgewählt sein.
Bestätigen Sie mit Klick auf **Weiter.**








Im nächsten Schritt werden Sie aufgefordert, Daten zum bestehenden Netzwerk und der Betriebsart einzustellen. Verwenden Sie hier als Band die Option **2.4 GHz (B+G),** den Modus **AP,** und als SSID die Bezeichnung Ihres neuen WLAN-Netzwerks (z.B. **ULF-1**).



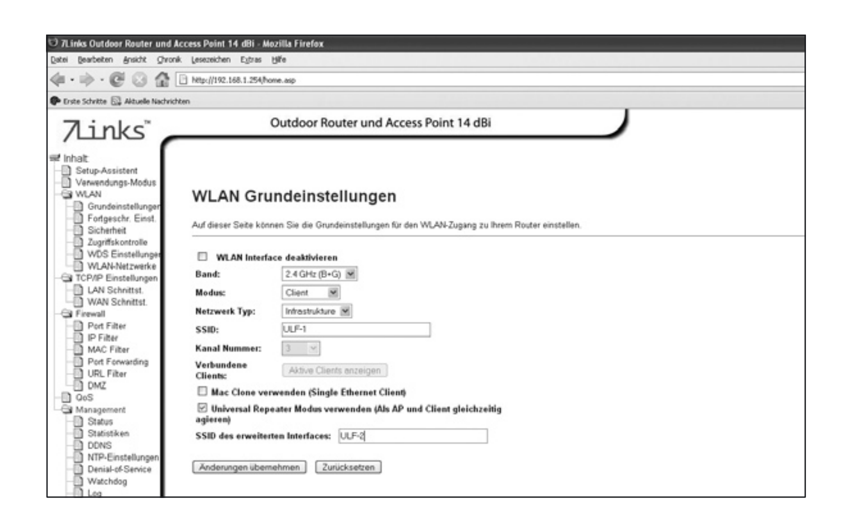
Der letzte Konfigurationsschritt dient zur Festlegung der Netzwerksicherheit. Stellen Sie hier als Verschlüsselung ◘ **keine** ein. Dies verhindert, dass es bei der ersten Verbindung Ihrer WLAN-Geräte in das neue WLAN-Netzwerk zu unvorhersehbaren Problemen kommt. Klicken Sie abschließend auf **Fertig stellen**, um die Erstkonfiguration abzuschließen.

*HINWEIS:*
*Nachdem Ihr Router in das Netzwerk eingebunden wurde und Sie Ihre WLAN-Geräte verbunden haben, wird empfohlen im Menüpunkt **Sicherheit** (Unterpunkt von **WLAN**) eine sichere Verschlüsselungsmethode festzulegen!*

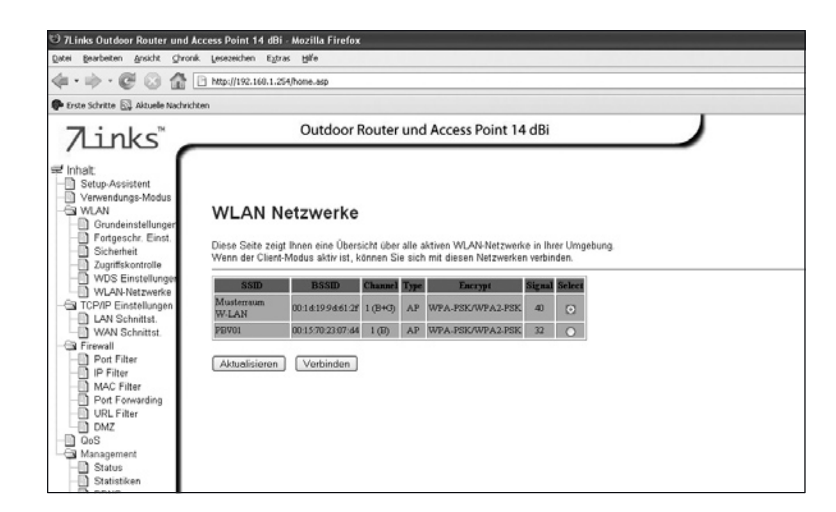
DEU

**Einbindung des vorkonfigurierten Servers ins Netzwerk**
Nachdem Sie den Router soweit vorbereitet haben, bringen Sie ihn wie im Punkt **Montage** (S.19)beschrieben an seiner Endposition an. Zur Endkonfiguration sollte der Computer, von dem aus konfiguriert wird, per LAN-Kabel an das Netzwerk mit Ihrem neuen WLAN-Router angeschlossen sein. Später kann die Konfiguration kabellos erfolgen.
Geben Sie nun in Ihrem Browser die neu zugewiesene IP-Adresse des Routers ein (in unserem Beispiel ist die die **192.168.1.2**).

- **Als Zweitrouter einbinden**
  Wenn Sie den Router als **Wireless ISP** eingerichtet haben, wählen Sie im Hauptmenü den Punkt **WLAN** und **Grundeinstellungen.**
  Aktivieren Sie hier den Punkt **Universal Repeater Modus verwenden** und geben Sie unter **SSID des erweiterten Interfaces** den Namen an, den Ihr neuer WLAN-Zugriffspunkt (der Router) für WLAN-Geräte anzeigen soll (z.B. **ULF-2**).



Klicken Sie anschließend im Hauptmenü auf **WLAN-Netzwerke.**
Klicken Sie nun auf **Aktualisieren**, um die verfügbaren WLAN-Netzwerke in Ihrer Umgebung anzeigen zu lassen. Wählen Sie aus der Liste Ihr bestehendes WLAN-Netzwerk aus (Sie erkennen Ihr Netzwerk an der verwendeten SSID).
Klicken Sie anschließend auf **Verbinden**.



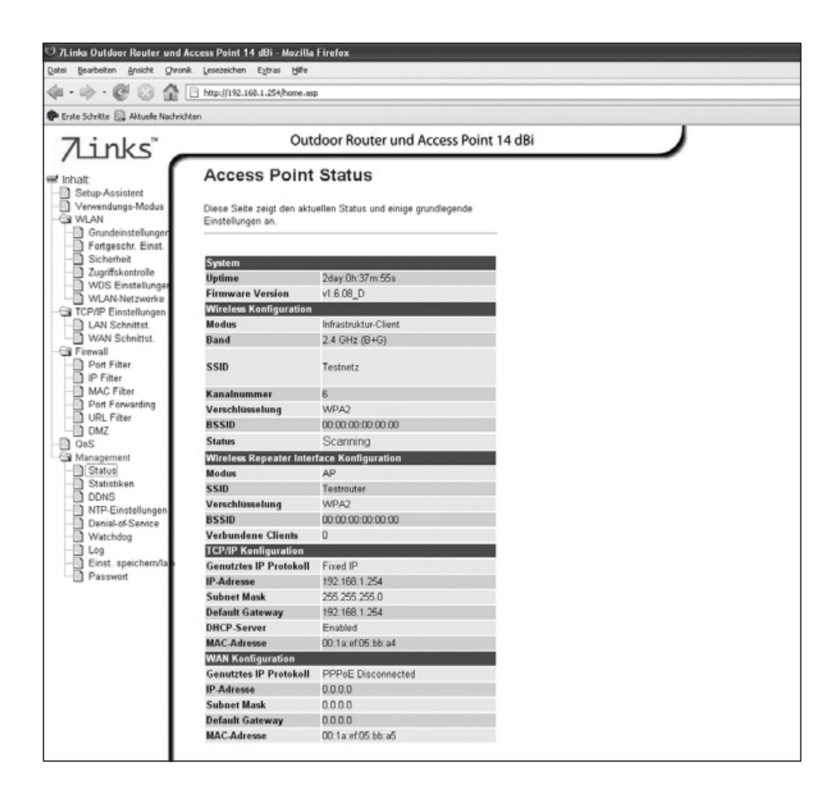

Erscheint die Meldung **Connect successfully,** war die Verbindung erfolgreich.





- **Als Einzelrouter einbinden**
  Wenn Sie den Router als **Gateway** eingerichtet haben, verbinden Sie das Netzwerkkabel zum DSL-Modem, Kabelmodem oder ähnlichen direkten Zugangsmöglichkeiten mit der POE-Box und das Verbindungskabel dann mit dem WAN-Port des Routers.

  Im Menübereich **Management** unter dem Unterpunkt **Status** können Sie anschließend überprüfen, ob die Verbindung zu Ihrem Internetanbieter erfolgreich war. Die Daten über die Verbindung mit Ihrem Internetanbieter werden im Bereich **WAN Konfiguration** angezeigt.



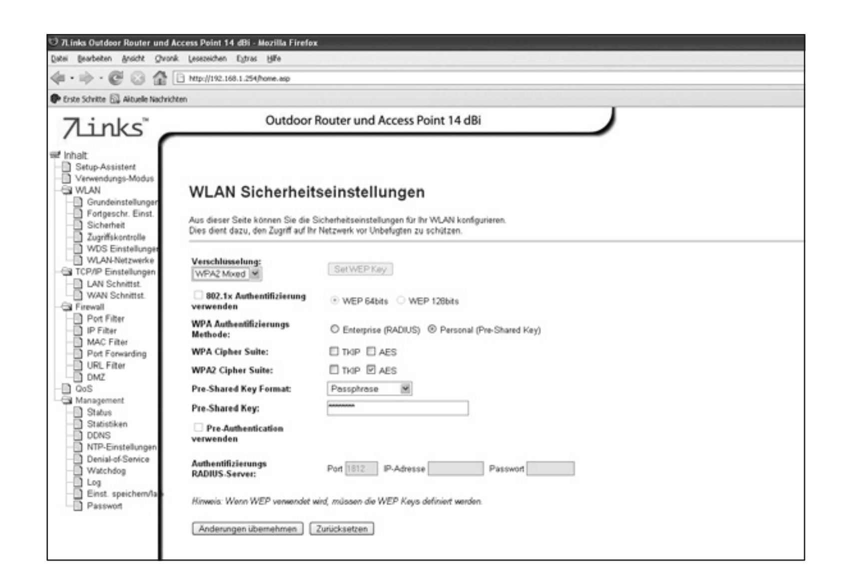
# SICHERHEITSEINSTELLUNGEN VORNEHMEN

Um den unberechtigten Zugriff auf Ihr Netzwerk zu verhindern, ist es notwendig, entsprechende Sicherheitsmaßnahmen zu ergreifen. Fremde Nutzer könnten sonst ungehindert auf Ihre Computer zugreifen, die sich im Netzwerk befinden.
Der sicherste Weg, Ihr WLAN-Netzwerk zu schützen, ist die Verwendung der WPA2-Verschlüsselung ◪ und die Zugangsbeschränkung nur für erlaubte MAC-Adressen.
Jedes Ihrer WLAN-Geräte besitzt eine einzigartige MAC-Adresse ◪ –vergleichbar mit einem Fingerabdruck.

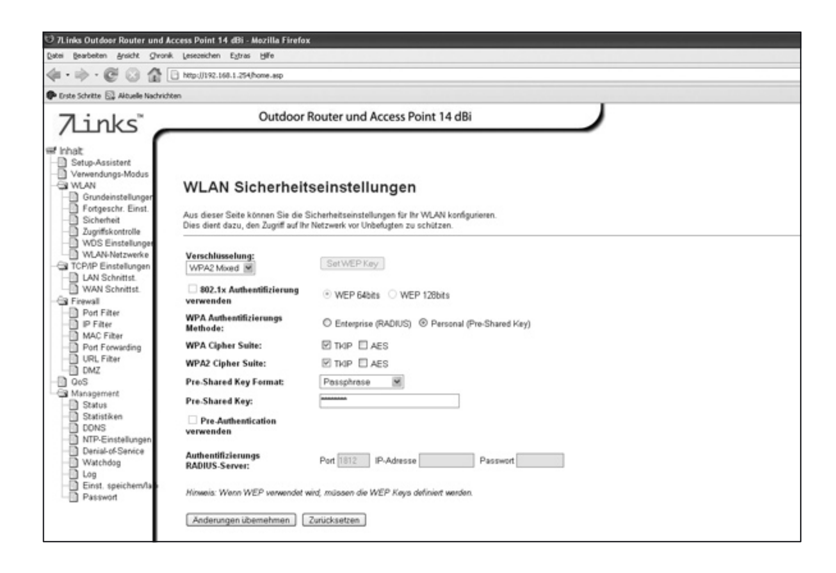
*HINWEIS:*
*Bevor Sie beginnen einzelne Geräte endgültig in Ihr WLAN-Netzwerk einzubinden, müssen zuerst die entsprechenden Sicherheitseinstellungen am Router vorgenommen werden.*

**Einrichten der WPA/WPA2-Verschlüsselung**
Rufen Sie in Ihrem Browser ◪ die Konfigurationseinstellungen Ihres Routers auf. Klicken Sie im Hauptmenü auf den Punkt **WLAN** und dann auf **Sicherheit.**

Wählen Sie als Verschlüsselung **WPA2 Mixed**. Damit stellen Sie sicher, dass auch ältere Geräte, die nur WPA-Verschlüsselung ◪ unterstützen ebenfalls mit Ihrem Netzwerk verbunden werden können.



Als nächstes nehmen Sie die Einstellungen zur WPA/WPA2-Verschlüsselung vor. Wählen Sie als Authentifizierungsmethode **Personal** und als **WPA/WPA2-Cipher-Suite** jeweils **TKIP.** Die Option **AES** sollten Sie nicht verwenden, da dies derzeit noch häufig zu Problemen beim Verbindungsaufbau zwischen zwei Geräten führt.

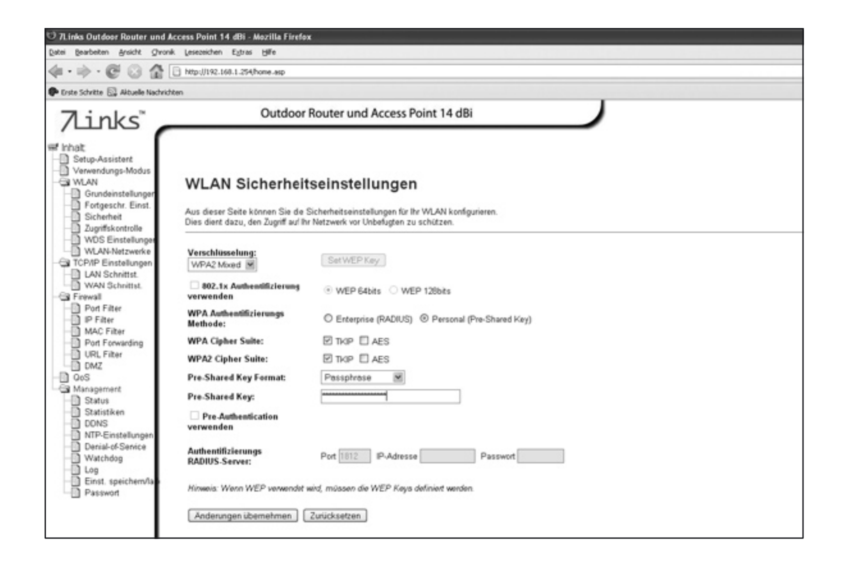



Nun wird noch ein Passwort für die Verbindung der Geräte benötigt. Stellen Sie hierzu bei **Pre-Shared Key Format** den Wert **Passphrase** ein.
Im Feld **Pre-Shared Key** geben Sie anschließend das Passwort ein, mit dem Sie den Zugang zu Ihrem Netzwerk sichern wollen.

*HINWEIS:*
*Ein Passwort sollte möglichst aus mehr als 6 Zeichen und einigen Sonderzeichen (z.B. @, $, ?, !, usw. ) bestehen. Notieren Sie sich das Passwort nötigenfalls und geben Sie dieses nicht an Außenstehende weiter.*








Speichern Sie die vorgenommenen Änderungen, mit Klick auf **Änderungen übernehmen**.

**Verwenden der MAC-Filterfunktion** Whitelist

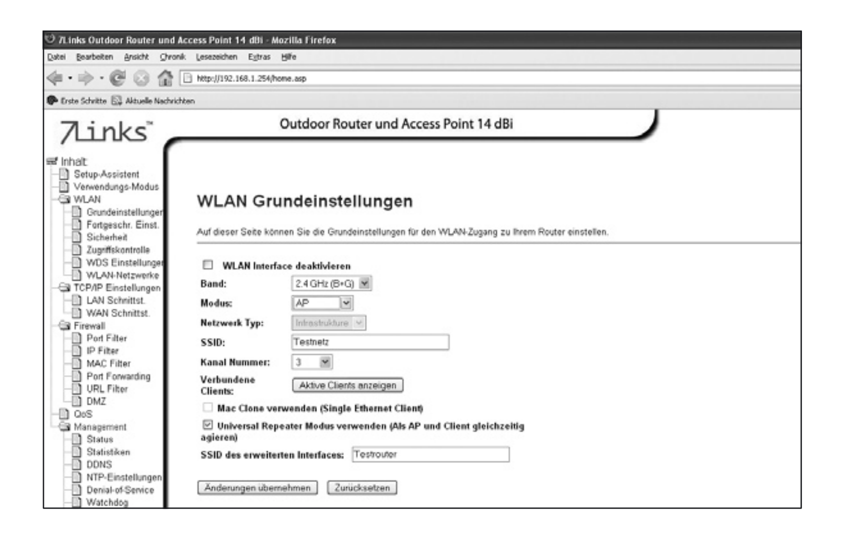
Die **Whitelist**-Filterfunktion für MAC-Adressen erlaubt nur ganz bestimmten, von Ihnen zugelassenen Geräten den Zugriff auf Ihr Netzwerk.

Bevor Sie jedoch damit beginnen, diese Zugriffseinschränkung zu verwenden, sollten Sie zuerst einmal die MAC-Adressen ➘ aller Ihrer WLAN-Geräte zu notieren.

Die einfachste Möglichkeit, die MAC-Adressen Ihrer Geräte zu ermitteln besteht darin, alle Geräte, die künftig in Ihrem WLAN-Netzwerk genutzt werden sollen, nacheinander mit dem Router zu verbinden.

*HINWEIS:*
*Der nächste Schritt kann nur ausgeführt werden, wenn der Router im Access-Point Modus eingestellt ist. Ist dies nicht der Fall, entnehmen Sie die MAC-Adressen der einzelnen Gerät bitte den jeweiligen Unterlagen der Geräte.*

Wenn Sie alle Geräte verbunden haben, klicken Sie im Hauptmenü der Routerkonfiguration auf **WLAN** und anschließend auf **Grundeinstellungen.**



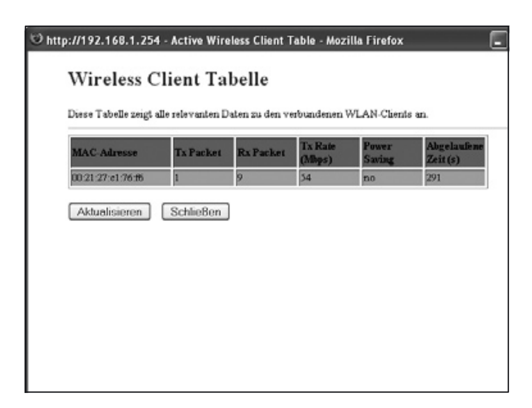





Klicken Sie nun auf der Button **Aktive Clients➘ anzeigen**.

In dieser Übersicht werden alle derzeit mit dem Router verbundenen Geräte mit Ihrer MAC-Adresse ➘ aufgelistet.

Notieren Sie sich diese Adressen.



http://192.168.1.254 - Active Wireless Client Table - Mozilla Firefox

Wireless Client Tabelle

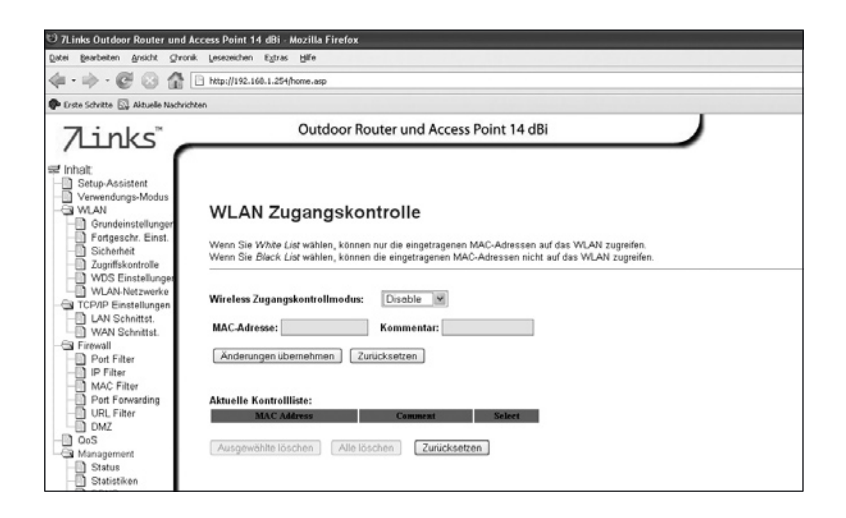
Diese Tabelle zeigt alle relevanten Daten zu den verbundenen WLAN-Clients an.

| MAC-Adresse | Tx Packet | Rx Packet | Tx Rate (Mbps) | Power Saving | Abgelaufene Zeit (s) |
|---|---|---|---|---|---|
| 00:21:27:e1:76:f6 | 1 | 9 | 54 | no | 291 |

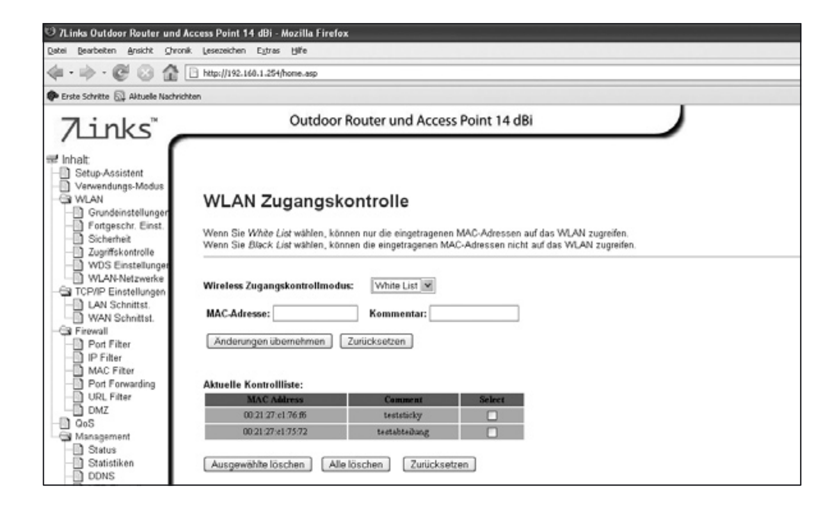
Aktualisieren Schließen

Schließen Sie das Fenster der Clientübersicht wieder.

Wählen Sie im Hauptmenü **WLAN** und den Unterpunkt **Zugriffskontrolle.**



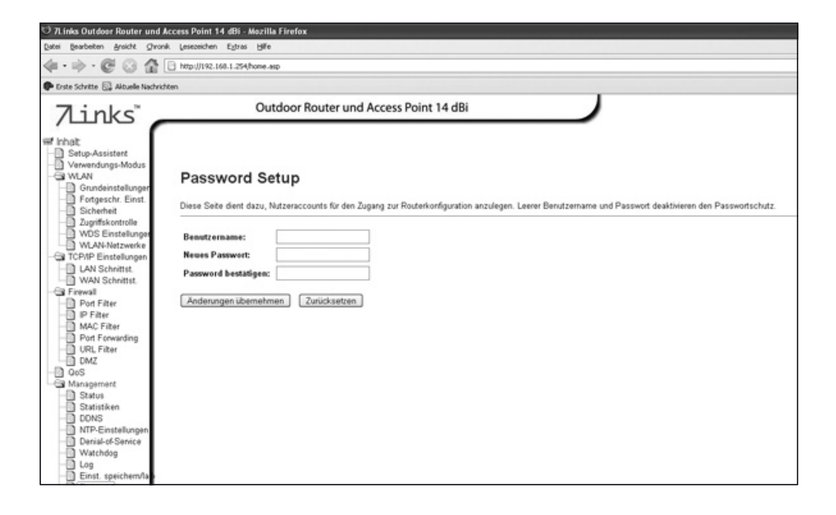
Stellen Sie nun den **Wireless Zugangskontrollmodus** auf den Wert **White List** ▾ ein.
Geben Sie nun nacheinander im Feld **MAC-Adresse** die MAC-Adresse Ihrer Geräte ein (ohne Doppelpunkte) und versehen Sie diese jeweils im Kommentarfeld mit einer sinnvollen Gerätebezeichnung (z.B. Notebook, Handy, usw.).
Speichern Sie jeden Eintrag mit Klick auf **Änderungen übernehmen**.








**Den Router mit einem Passwort sichern**
Um Ihren Router gegen unbefugten Zugriff auf die Konfigurationseinstellungen zu sichern, ist es notwendig, diesen mit einem Passwortschutz abzusichern.
Klicken Sie dazu im Hauptmenü der Routerkonfiguration auf **Management** und den Unterpunkt **Passwort.**




Geben Sie hier einen Benutzernamen für den Zugang an und ein zugehöriges Passwort. Bestätigen Sie die Eingaben mit Klick auf **Änderungen übernehmen**.

*HINWEIS:*
*Verwenden Sie möglichst nicht Ihren realen Namen als Benutzernamen, und ein sicheres Passwort. Ein Passwort sollte möglichst aus mehr als 6 Zeichen und einigen Sonderzeichen (z.B. @, $, ?, !, usw. ) bestehen. Notieren Sie sich das Passwort nötigenfalls und geben Sie dieses nicht an Außenstehende weiter.*

# ABSCHLIESSENDE WORTE

Sie haben Ihren neuen WLAN-Router nun in Ihr Netzwerk eingebunden und nach heute gängigen Sicherheitsmaßstäben gegen unbefugten Zugriff gesichert. Vielleicht sind Ihnen jedoch noch immer einige Begriffe oder Zusammenhänge aus dieser Anleitung unklar, oder nur in Ansätzen bekannt. Daher werden zur weiteren Lektüre über die Themen Netzwerke, WLAN und deren Sicherheit folgende Titel auf www.pearl.de empfohlen:

| | |
|---|---|
| CL-945 | Heimnetzwerke mit DSL & WLAN |
| PK-3915 | Handbuch Heimnetzwerke |



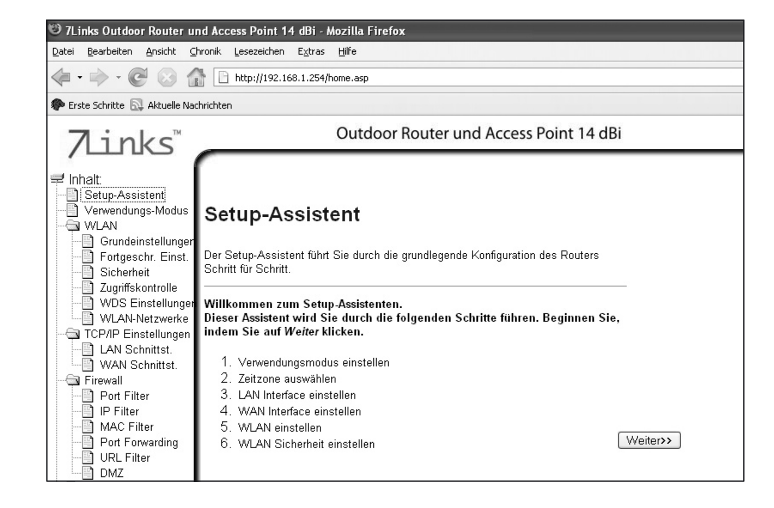




# DETAILLIERTE ERLÄUTERUNGEN ZUR KONFIGURATION

# SCHNELLKONFIGURATION

Bereiten Sie die Montage des Routers wie auf den Seiten 19 ff. beschrieben vor. Schließen Sie den Router zur Vorbereitung per Kabel an einen einzelnen Rechner an. Rufen Sie dann über einen Webbrowser die Konfigurationsseite des Routers auf. Geben Sie dazu die werkseitige IP-Adresse des Routers ein (**192.168.1.254**).
Die Konfigurationsseite startet direkt mit dem Konfigurationsassistenten.




Verwenden Sie den Assistenten, um die grundlegenden Einstellungen schnell und unkompliziert vorzunehmen.
Die drei einstellbaren Verwendungsmodi können kurz folgendermaßen unterschieden werden:

| | |
|---|---|
| **Gateway** | Der Router wird als Hauptrouter (oder einziger) verwendet, WAN- und NAT-Funktionen werden verwendet. |
| **Bridge** | Die Verbindungen des Routers werden nur für den Intranetverkehr freigegeben, NAT- und WAN-Funktionen werden nicht verwendet. |
| **Wireless ISP** | Wird verwendet, wenn der Router über einen zweiten WLAN-Router ans Internet angebunden werden soll. |





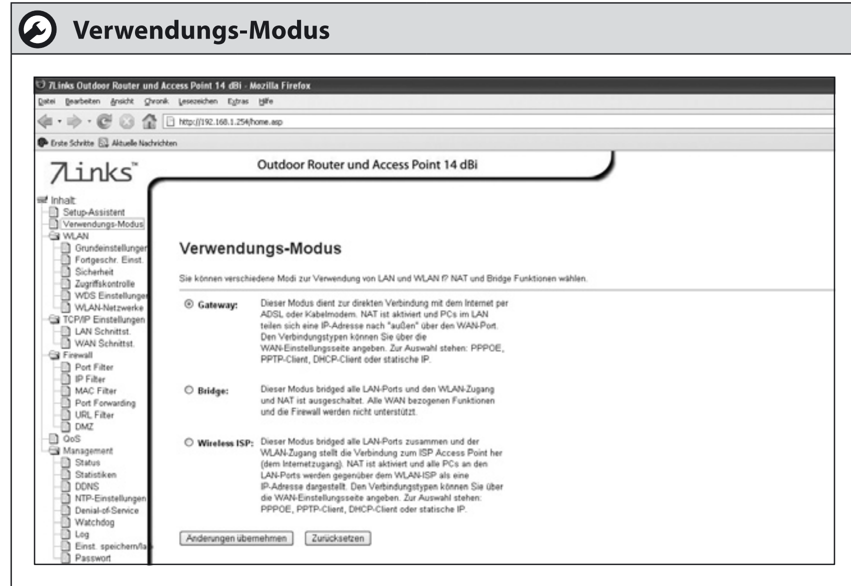
Anschließend können Sie einen NTP-Server einstellen.
Im nächsten Schritt geben Sie die LAN-IP und deren Subnetzmaske ein, die der Router später verwenden soll.
Der vierte Schritt wird zur Konfiguration des WAN-Interface verwendet. Das Interface wird je nach Nutzungsart entweder per WAN-Port und Kabel (**Gateway**) oder per WLAN (**Wireless ISP**) verwendet. Geben Sie daher entsprechend der Anbindung die nötigen Informationen ein.
Der Punkt **Wireless Grundeinstellungen** wird zur Konfiguration der WLAN-Schnittstelle verwendet.
Beim letzten Punkt können Sie einen Verschlüsselungstyp für Ihr Netzwerk festlegen, jedoch sollten Sie bei der Vorkonfiguration darauf verzichten, um Fehlerquellen auszuschließen.

Nachdem Sie die Vorkonfiguration abgeschlossen haben, können Sie den Router am vorgesehenen Einsatzort anbringen.
Anschließend sollten Sie die endgültige Konfiguration vornehmen. Dies können Sie entweder per WLAN oder über den LAN-Zugang vornehmen.

*HINWEIS:*
*Achten Sie darauf, dass Sie die neu zugewiesene LAN-IP-Adresse zum Aufrufen der Konfigurationsseite verwenden.*

# SCHNELLREFERENZ DER KONFIGURATIONS-EINSTELLUNGEN MIT BEISPIELEN

Diese Referenz soll dem fortgeschrittenen Nutzer als Nachschlagewerk zu den einzelnen Menüpunkten und Einstellungsmöglichkeiten des WLAN-Routers dienen. Anwendungs- und Einsatzbeispiele geben dabei Aufschluss über mögliche Verwendungszwecke und veranschaulichen die einzelnen Vorgehensweisen.




| Option | Werte | Funktion |
|---|---|---|
| **Gateway** | Ein<br>Aus | Dieser Modus dient der direkten Verbindung des Routers mit dem Internet per DSL, PPPOE, Kabelmodem und anderen direkten Zugangsarten. NAT, Firewall, QoS und alle anderen relevanten Einstellungen können verwendet werden. |
| **Bridge** | Ein<br>Aus | Dieser Modus verbindet alle LAN-Ports und die WLAN-Schnittstelle und „bridged" sie auf einen zweiten Access-Point. NAT und Firewall-Funktionen sind inaktiv. |
| **Wireless ISP** | Ein<br>Aus | Dieser Modus funktioniert analog zur Bridge-Funktion. Allerdings werden NAT, Firewall, QoS und andere Einstellungen mitunterstützt. Dieser Modus empfiehlt sich dann, wenn das verwaltete WLAN-Netzwerk an ein Gateway angebunden werden soll. |

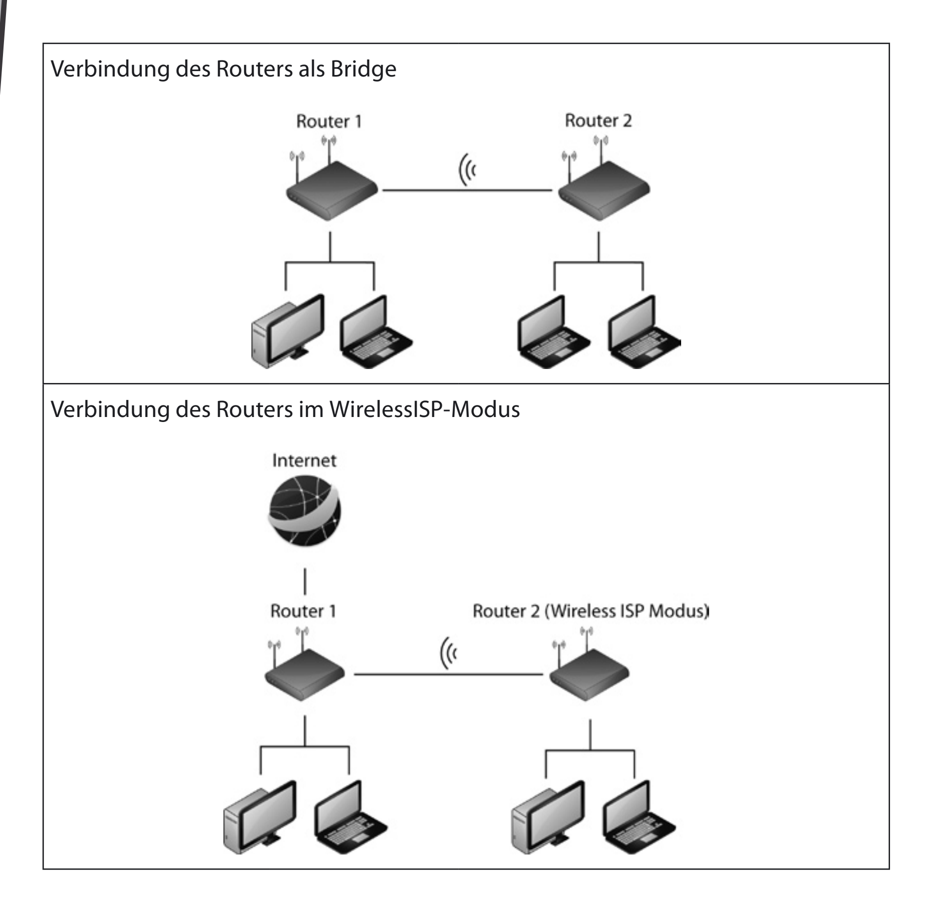
BEISPIELE

Verbindung des Routers als Gateway

Internet

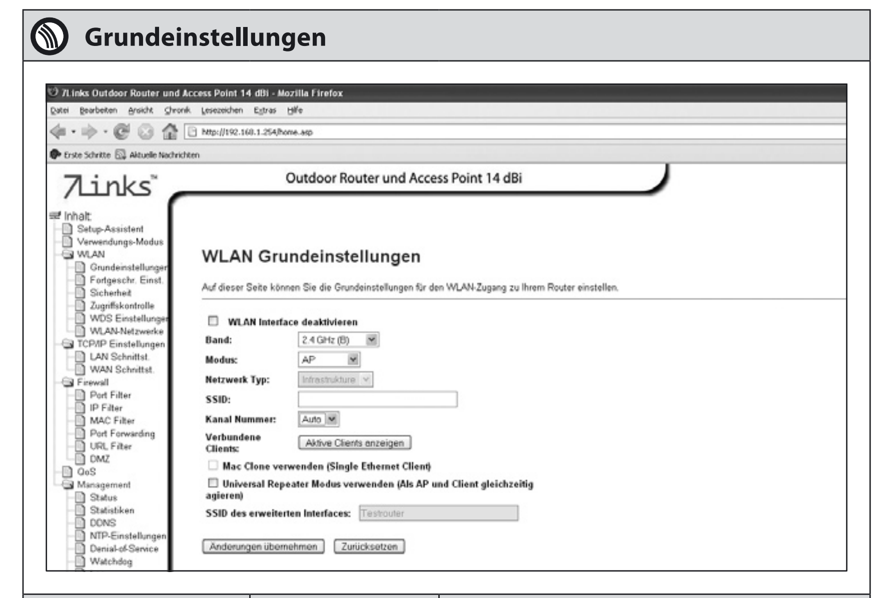
DSL-Modem

Router (Gateway)



# WLAN

## Grundeinstellungen

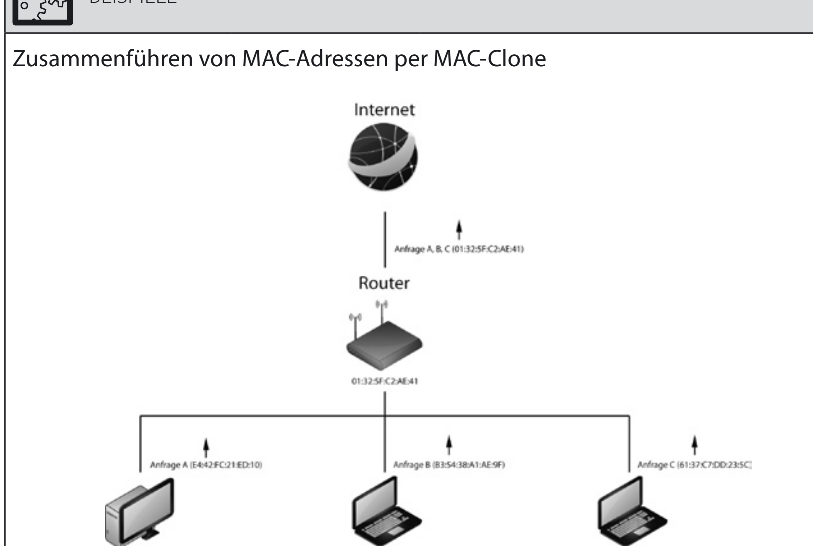



| Option | Werte | Funktion |
|---|---|---|
| **WLAN Interface deaktivieren** | Ein<br>Aus | Aktiviert oder deaktiviert die WLAN-Funktion des Routers. |
| **Band** | 2,4 GHz (B)<br>2,4 GHz (G)<br>2,4 GHz (B+G) | Einstellung der verwendeten WLAN-Bänder. |
| **Modus** | AP<br>Client<br>WDS<br>AP+WDS | Konfigurieren der Verwendungsart der WLAN-Schnittstelle.<br>Bei **Wireless ISP** muss **Client** aktiviert sein. |
| **Netzwerk Typ** | Infrastruktur<br>Ad Hoc | Feste oder variable Netzwerkstruktur |
| **SSID** | <text> | Bezeichnung des Netzwerks |
| **Kanal Nummer** | Auto<br>1-11 | Kanal der für WLAN verwendet werden soll |
| **Mac Clone verwenden** | Ein<br>Aus | Vergleichbar mit NAT, werden sich im Netzwerk befindliche Geräte nach „außen“ mit der gleichen MAC-Adresse dargestellt. |

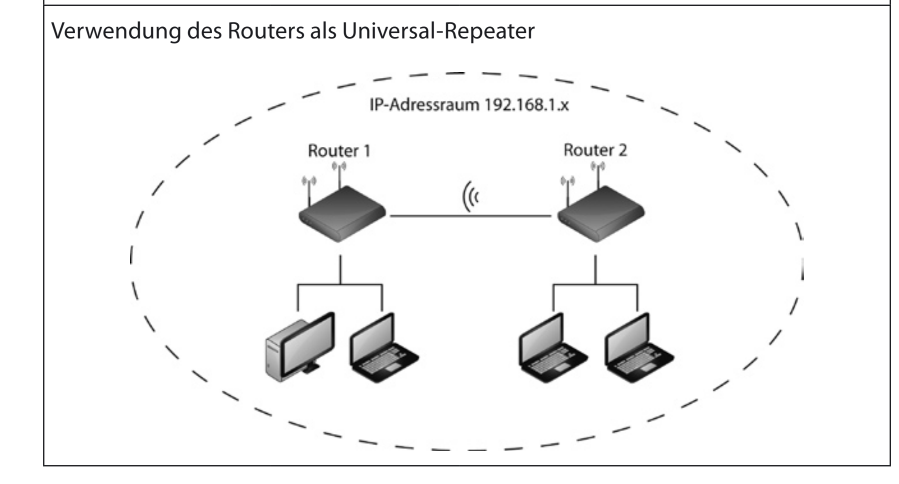
| | | |
|---|---|---|
| **Universal Repeater Modus verwenden** | Ein<br>Aus | Wenn dieser Punkt aktiv ist, agiert die WLAN-Schnittstelle gleichzeitig im AP und Client Modus. Diese Einstellung ist spezielle für den Einsatz als im **Wireless ISP**-Modus von Bedeutung. |
| **SSID des erweiterten Interfaces** | <text> | Bezeichnung des erweiterten Netzwerks, wenn der **Universal Repeater Modus** verwendet wird. |

BEISPIELE

Zusammenführen von MAC-Adressen per MAC-Clone




Verwendung des Routers als Universal-Repeater

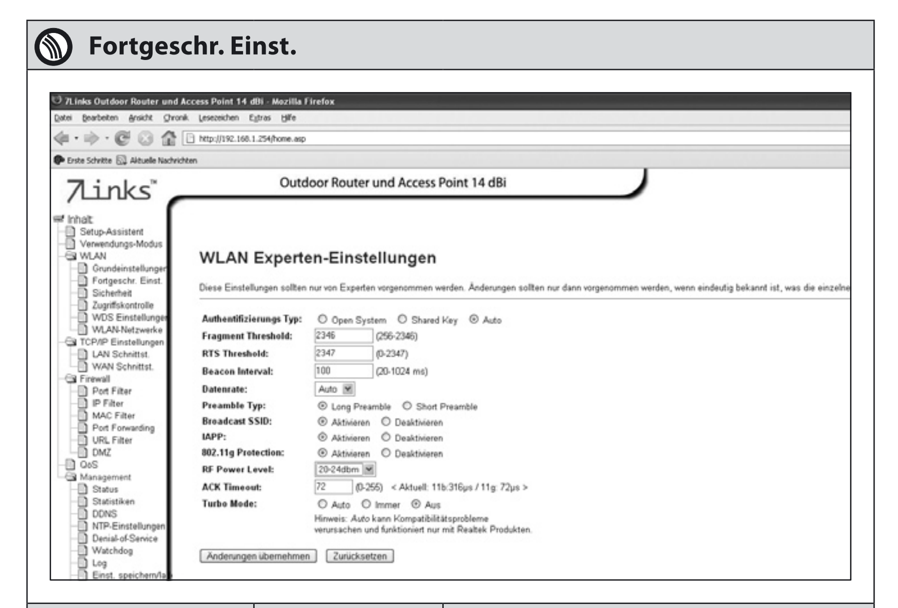








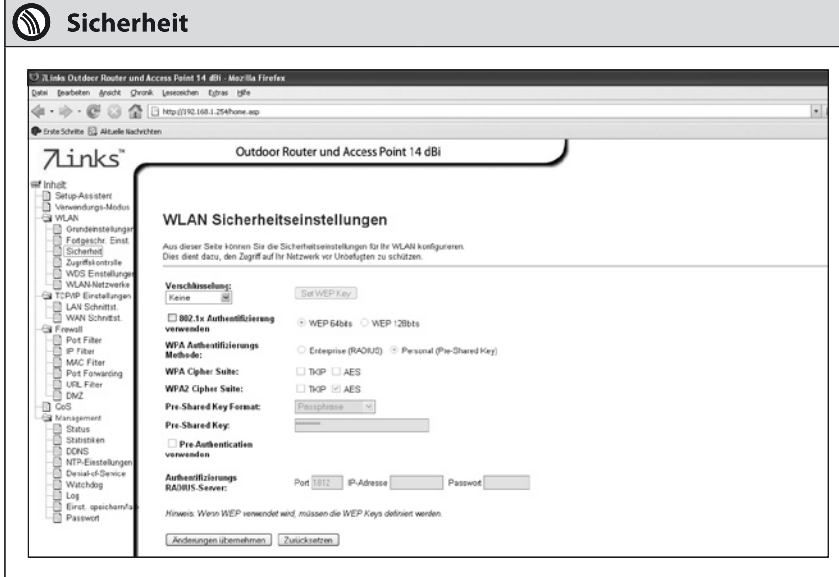

## Fortgeschr. Einst.




| Option | Werte | Funktion |
|---|---|---|
| **Authentifizierungs Typ** | Open System<br>Shared Key<br>Auto | Einstellung der Authentifizierungs-methode. Kann fest vorgegeben werden oder automatisch übernommen werden. |
| **Fragement Threshold** | 256-2346 | Fragmentierungsschwellwert der verwendeten Datenpakete. Bei schlechter Verbindung kann ein niedrigerer Wert die Übertragungsqualität verbessern. |
| **RTS Threshold** | 0-2347 | Schwellwert für Handshake-Anfragen zur Kollisionsvermeidung. |
| **Beacon Intervall** | 20-1024 | Synchronisationsintervall der WLAN-Schnittstelle. |
| **Datenrate** | Auto<br>1M-54M | Festlegen der zu verwendenden Datenübertragunsgeschwindigkeit. |
| **Preamble Typ** | Long<br>Short | Größe der CRC-Datenpakete. |
| **Broadcast SSID** | Ein<br>Aus | SSID öffentlich ausstrahlen oder verbergen. |
| **IAPP** | Ein<br>Aus | Verwenden des **Inter Access Point Protokolls** (Roaming zwischen Access-Points) |
| **802.11g Protection** | Ein<br>Aus | Wenn aktiviert, können sowohl 802.11b als auch 802.11g Geräte im gleichen Netzwerk verwendet werden. |

| | | |
|---|---|---|
| **ACK Timeout** | 0-255 | Zeit die bis zur Rückmeldung im WLAN maximal vergehen darf. |
| **Turbo Mode** | Auto<br>Immer<br>Aus | Bei Realtek WLAN Chipsätzen kann durch den Turbo Mode eine höhere Datentransferrate erzielt werden.<br>Bei anderen Chipsätzen kann dies zu Kompatibilitätsproblemen führen. |

## Sicherheit




| Option | Werte | Funktion |
|---|---|---|
| **Verschlüsselung** | Keine<br>WEP<br>WPA<br>WPA2<br>WPA Mixed | Einstellen der verschiedenen Verschlüsselungsmethoden.<br>Wird **WEP** verwendet, können unter **Set WEP Key** die Schlüssel eingestellt werden. |
| **802.1x Authentifizierung verwenden** | Ein<br>Aus<br>64 Bit<br>128 Bit | Einstellen der Schlüssellänge bei der Verwendung von **WEP**. |
| **WPA Authenti-fizierungs Methode** | Enterprise<br>Personal | Einstellen, ob ein RADIUS-Server verwendet wird, oder die Authentifzierung per Pre-Shared-Key vorgenommen werden soll. |
| **WPA Cipher Suite** | TKIP<br>AES | Einstellen welche WPA Cipher verwendet werden. |
| **WPA2 Cipher Suite** | TKIP<br>AES | Einstellen, welche WPA2 Cipher verwendet werden. |

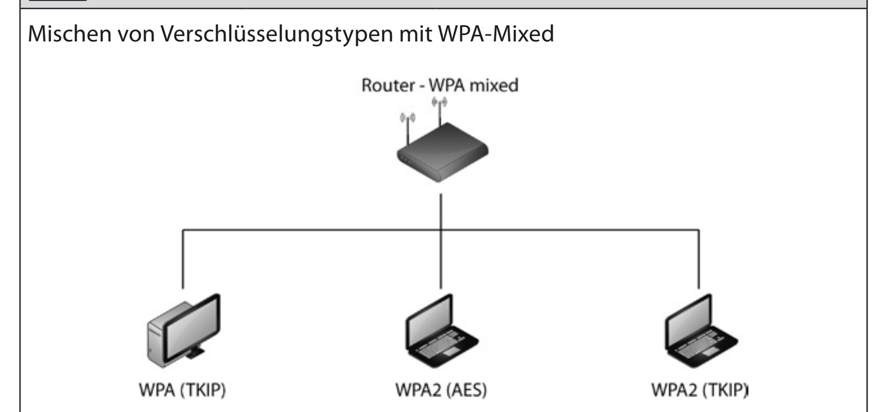




| | | |
|---|---|---|
| **Pre-Shared Key Format** | Passphrase<br>Hex | Einstellen ob der Pre-Shared-Key im Klartext oder als Hex-Wert abgefragt wird. |
| **Pre-Shared Key** | <text><br><hexcode> | Einstellen des verwendeten Schlüssels. |
| **Pre-Authentication verwenden** | Ein<br>Aus | Wird speziell für Roaming verwendet. |
| **Authenti-fizierungs RADIUS-Server** | <text> | Verbindungsdaten des verwendeten RADIUS-Servers. |

BEISPIELE

Mischen von Verschlüsselungstypen mit WPA-Mixed



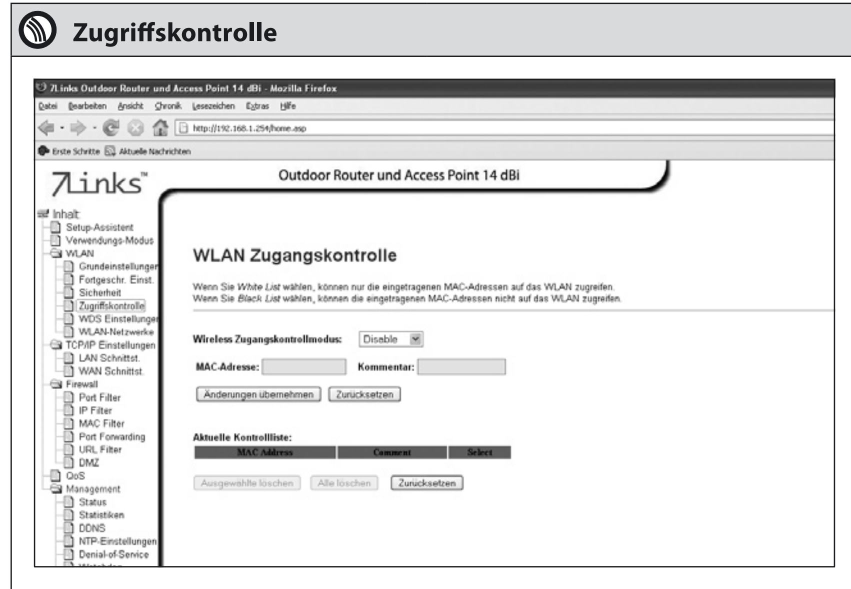

Verschlüsselungsverwaltung per RADIUS-Server

RADIUS-Server

WPA-Auth.

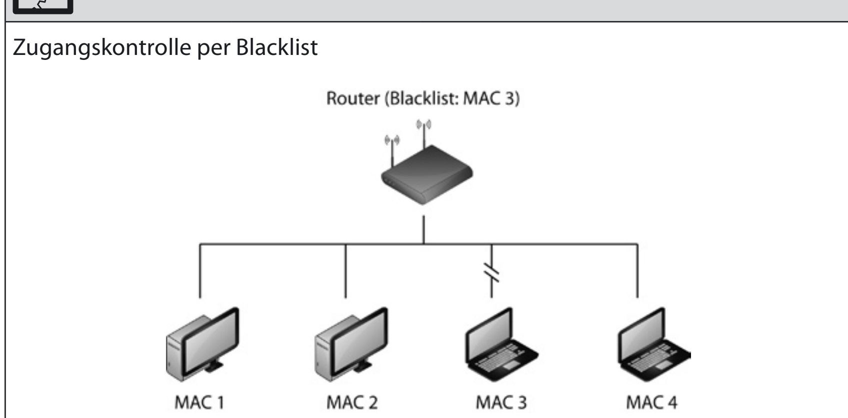
WPA-Auth.

## Zugriffskontrolle



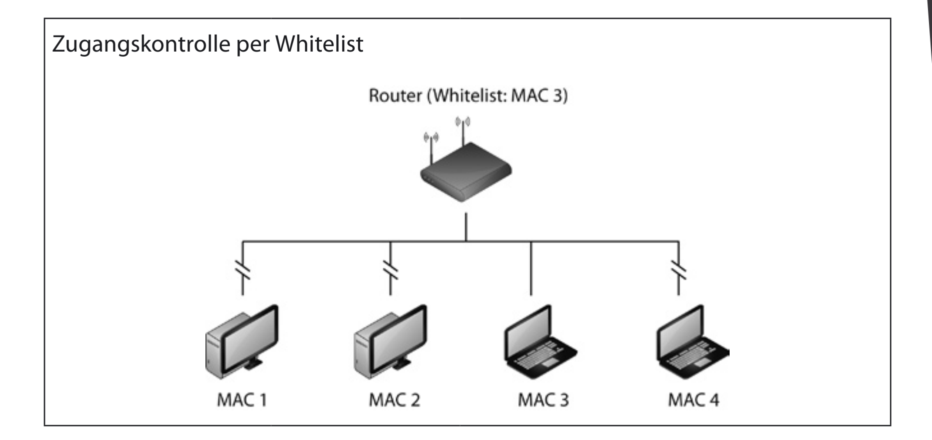

| Option | Werte | Funktion |
|---|---|---|
| **Wireless Zugangs-kontrollmodus** | Deaktiviert<br>White List<br>Black List | Einstellen der verwendeten Zugangskontrolle. |
| **MAC-Adresse** | <text> | Die betreffende MAC-Adresse |
| **Kommentar** | <text> | Kommentar |

BEISPIELE

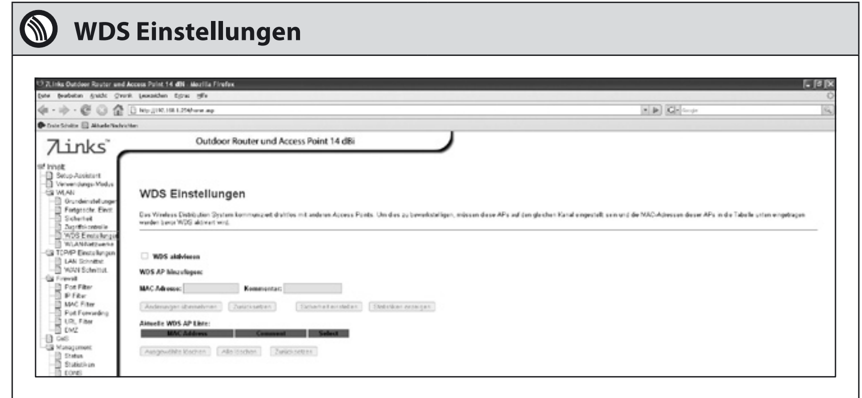






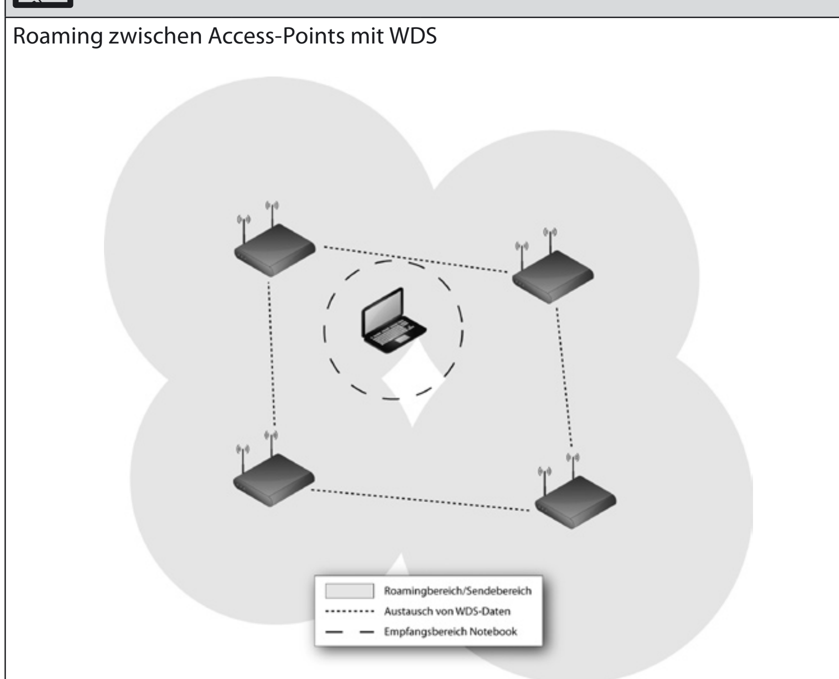
## WDS Einstellungen




| Option | Werte | Funktion |
|---|---|---|
| **WDS aktivieren** | Ein<br>Aus | Aktivieren des Wireless Distribution Systems (verteilte Access-Points). |
| **MAC-Adresse** | <text> | MAC-Adresse eines Access-Points |
| **Kommentar** | <text> | Kommentar |

BEISPIELE

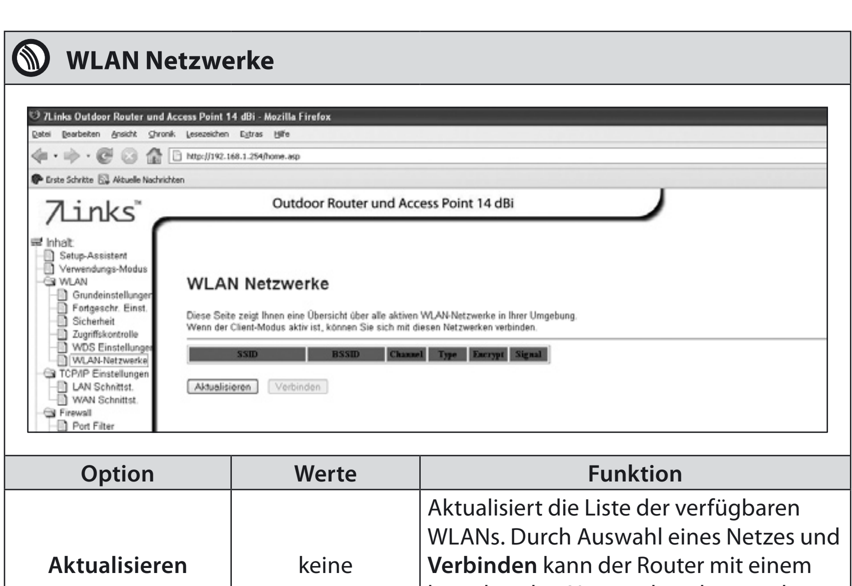
Roaming zwischen Access-Points mit WDS



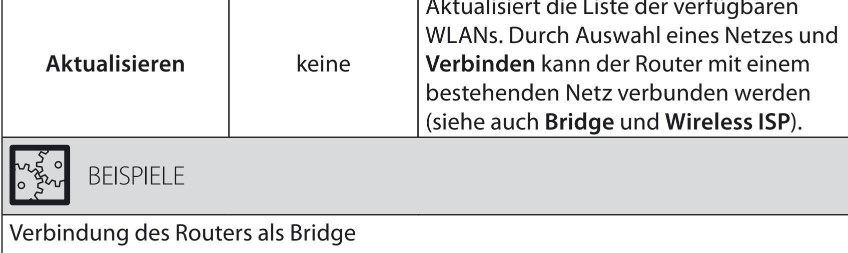




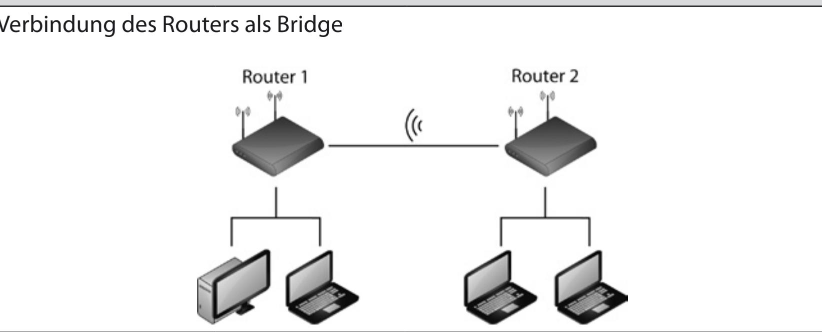

## WLAN Netzwerke




| Option | Werte | Funktion |
|---|---|---|
| **Aktualisieren** | keine | Aktualisiert die Liste der verfügbaren WLANs. Durch Auswahl eines Netzes und **Verbinden** kann der Router mit einem bestehenden Netz verbunden werden (siehe auch **Bridge** und **Wireless ISP**). |

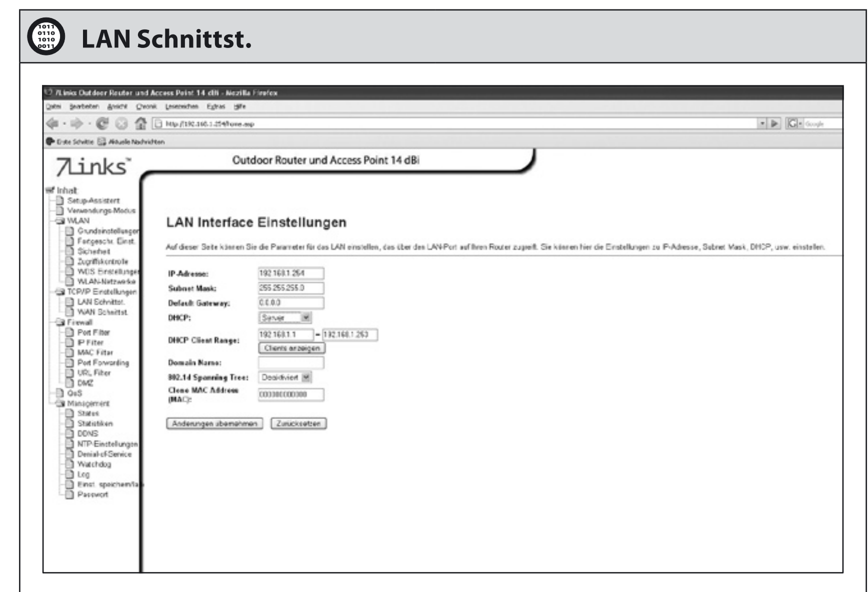

BEISPIELE

Verbindung des Routers als Bridge



# TCP/IP EINSTELLUNGEN

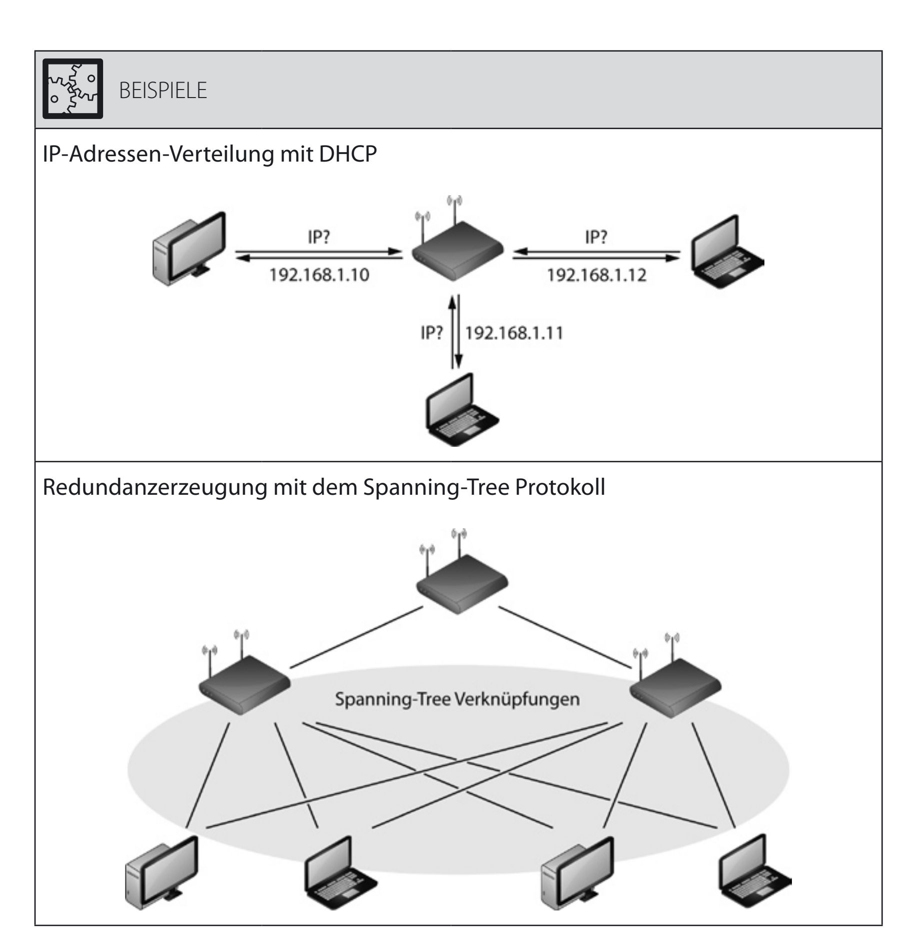
## LAN Schnittst.




| Option | Werte | Funktion |
|---|---|---|
| **IP-Adresse** | <text> | IP-Adresse, mit der der Router über die LAN-Schnittstelle angesprochen werden kann. |
| **Subnet Mask** | <text> | Zu verwendende Subnetz-Maske. |
| **Default Gateway** | <text> | Zu verwendendes Gateway. Entweder IP-Adresse des ISP oder des Hauptrouters. |
| **DHCP** | Deaktiviert<br>Client Server | Regelt die Verwendung von DHCP über den Router (automatische IP-Adressen-Vergabe). |
| **DHCP-Client Range** | <text><br><text> | Einstellen des zu vergebenden IP-Adressbereichs. |
| **Domain Name** | <text> | Einstellen des Domain-Präfixes. |
| **802.1d Spanning Tree** | Ein<br>Aus | Verwendung des Spanning Tree Protokolls. |
| **Clone MAC Address** | <hexcode> | MAC-Adresse, die für das „cloning" intern verwendet werden soll. |







## WAN Schnittst.

| Option | Werte | Funktion |
|---|---|---|
| **WAN Zugangsart** | Statische IP<br>DHCP Client<br>PPPoE<br>PPTP | Einstellen des Verbindungstyps der WAN-Schnittstelle. |
| **IP-Adresse** | <text> | IP-Adresse, mit der der Router über die WAN-Schnittstelle angesprochen werden kann. |
| **Subnet Mask** | <text> | Zu verwendende Subnetz-Maske. |
| **Default Gateway** | <text> | Zu verwendendes Gateway. IP-Adresse des ISP. |
| **MTU Größe** | 1360-1500 | Maximale Paketgröße. |
| **Host Name** | <text> | Bezeichnung des Routers. |
| **Benutzername** | <text> | Benutzername zur Anmeldung beim ISP. |
| **Passwort** | <text> | Passwort zur Anmeldung beim ISP. |
| **Service Name** | <text> | Dialstring (falls erforderlich). |
| **Verbindungstyp** | Kontinuierlich<br>Connect on Demand<br>Manuell | Art des Verbindungsaufbaus. |
| **Idle Time** | 1-1000 | Zeit bis zum Verbindungsabbruch, wenn kein Datenverkehr mehr stattfindet. |
| **MPPE Verschlüsselung anfordern** | Ein<br>Aus | Microsoft Punkt-zu-Punkt-Verschlüsselung verwenden. |







| | | |
|---|---|---|
| **DNS automatisch beziehen** | Ein<br>Aus | Beziehen der DNS-IPs vom Gateway. |
| **DNS manuell einstellen** | Ein<br>Aus | Manuelle Angabe der DNS-IPs. |
| **DNS 1-3** | <text> | IP-Adressen der zu verwendenden DNS-Server. |
| **Clone MAC Address** | <text> | MAC-Adresse, die für das „cloning" extern verwendet werden soll. |
| **uPNP verwenden** | Ein<br>Aus | uPNP-Verwendung erlauben. |
| **Ping Access on WAN verwenden** | Ein<br>Aus | Ping-Anfragen auf den Router erlauben. |
| **Web Server Access on WAN** | Ein<br>Aus | Webserver-Anfragen vom WAN aus erlauben. |
| **IPsec pass through bei VPN Verbindungen verwenden** | Ein<br>Aus | Sichere VPN Verbindungen von einzelnen Clients zulassen. |
| **PPTP pass through bei VPN Verbindungen verwenden** | Ein<br>Aus | Sichere VPN Verbindungen von einzelnen Clients zulassen. |
| **L2TP pass through bei VPN Verbindungen verwenden** | Ein<br>Aus | Sichere VPN Verbindungen von einzelnen Clients zulassen. |

BEISPIELE

VPN-Tunnel zwischen zwei Netzwerken

Anbindung an einen ADSL-IPS (z.B. T-Online)

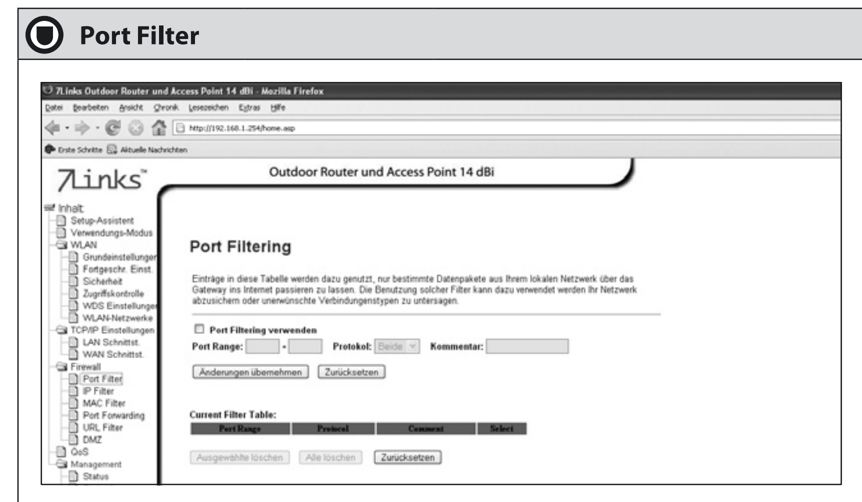
T-Online Router

DSL-Modem

Router (Gateway)

# FIREWALL

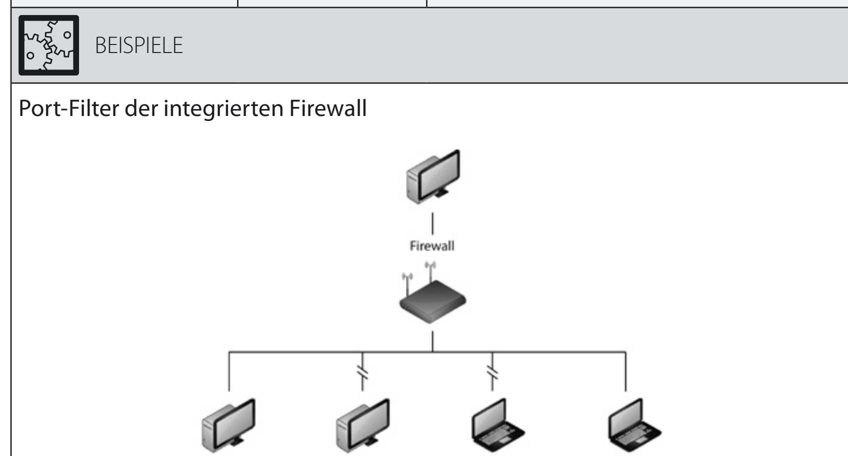
## Port Filter




| Option | Werte | Funktion |
|---|---|---|
| **Port Filtering verwenden** | Ein<br>Aus | Filter aktivieren |
| **Port Range** | <text><br><text> | Auf diese Ports anwenden |
| **Protokoll** | Beide<br>TCP<br>UDP | Auf diese/s Protokoll/e anwenden |
| **Kommentar** | <text> | Kommentar |

BEISPIELE

Port-Filter der integrierten Firewall



## IP Filter

Outdoor Router und Access Point 14 dBi

IP Filtering

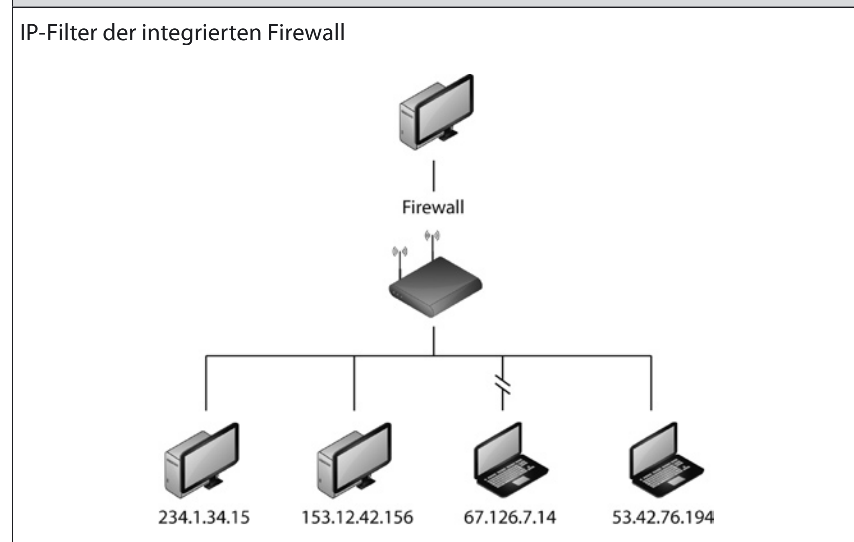
Einträge in diese Tabelle werden dazu genutzt, nur bestimmte Datenpakete aus Ihrem lokalen Netzwerk über das Gateway ins Internet passieren zu lassen. Die Benutzung solcher Filter kann dazu verwendet werden Ihr Netzwerk abzusichern oder unerwünschte Verbindungstypen zu untersagen.

IP-Filter verwenden
Lokale IP-Adresse: Protokol: Beide Kommentar:
Änderungen übernehmen | Zurücksetzen
Aktuelle Filter-Tabelle:
Local IP Address | Protocol | Comment | Select
Ausgewählte löschen | Alle löschen | Zurücksetzen

| Option | Werte | Funktion |
|---|---|---|
| **IP-Filter verwenden** | Ein<br>Aus | Filter aktivieren |
| **Lokale IP-Adresse** | <text> | Für diese IP-Adresse anwenden |
| **Protokoll** | Beide<br>TCP<br>UDP | Auf diese/s Protokoll/e anwenden |
| **Kommentar** | <text> | Kommentar |

BEISPIELE

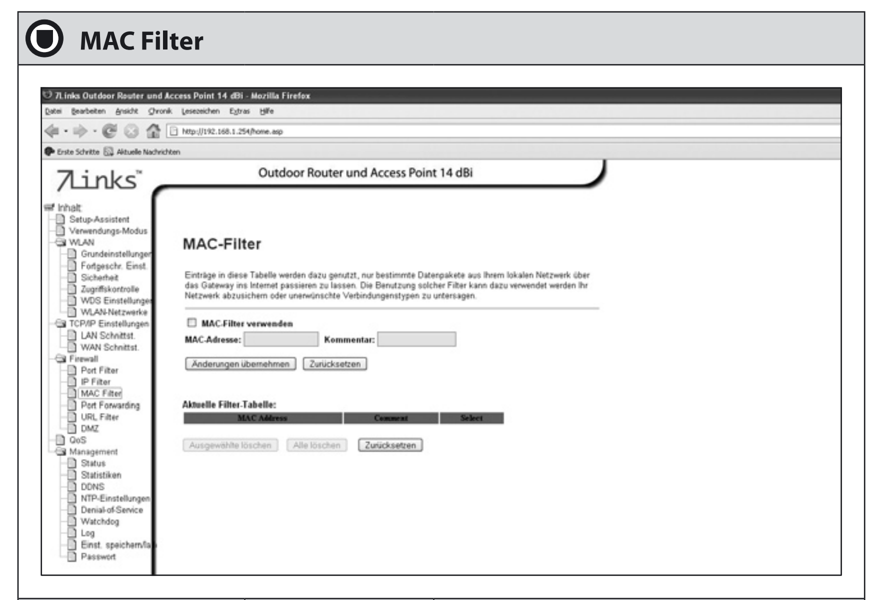
IP-Filter der integrierten Firewall







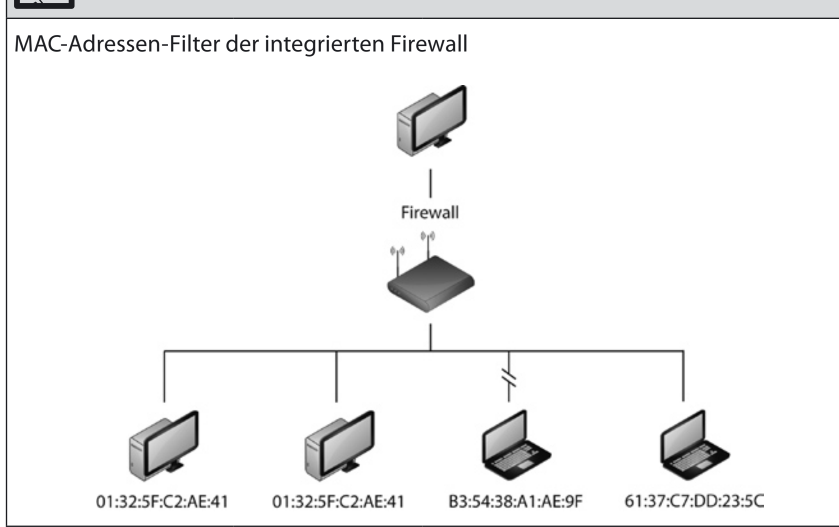

## MAC Filter



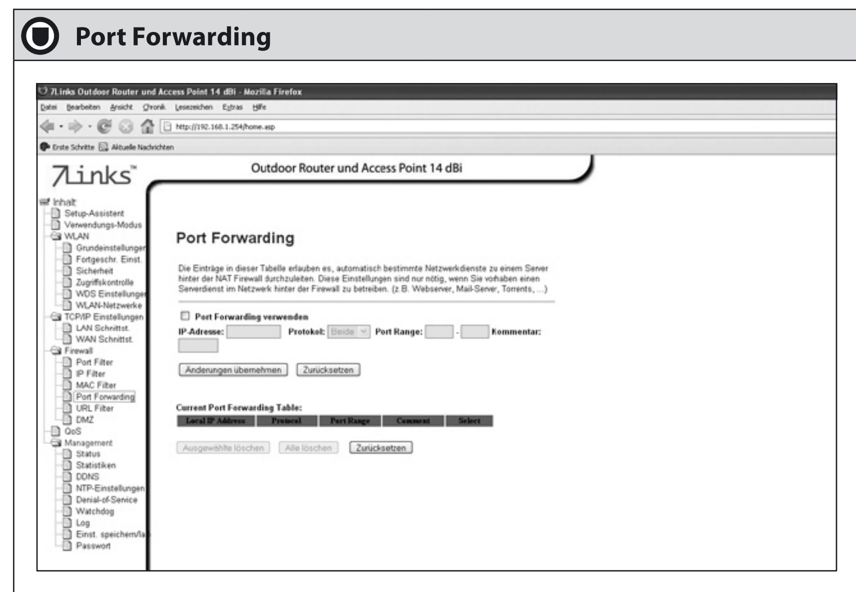

| Option | Werte | Funktion |
|---|---|---|
| **MAC-Filter verwenden** | Ein<br>Aus | Filter aktivieren |
| **MAC-Adresse** | <text> | Für diese MAC-Adresse anwenden |
| **Kommentar** | <text> | Kommentar |

BEISPIELE

MAC-Adressen-Filter der integrierten Firewall



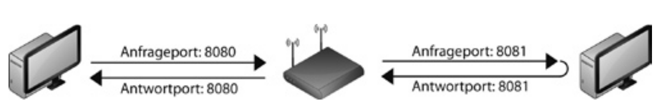
## Port Forwarding




| Option | Werte | Funktion |
|---|---|---|
| **Port Forwarding verwenden** | Ein<br>Aus | Forwarding aktivieren |
| **IP-Adresse** | <text> | Für diese IP-Adresse anwenden |
| **Protokoll** | Beide<br>TCP<br>UDP | Auf diese/s Protokoll/e anwenden |
| **Port Range** | <text><br><text> | Für diese Ports anwenden |
| **Kommentar** | <text> | Kommentar |

BEISPIELE

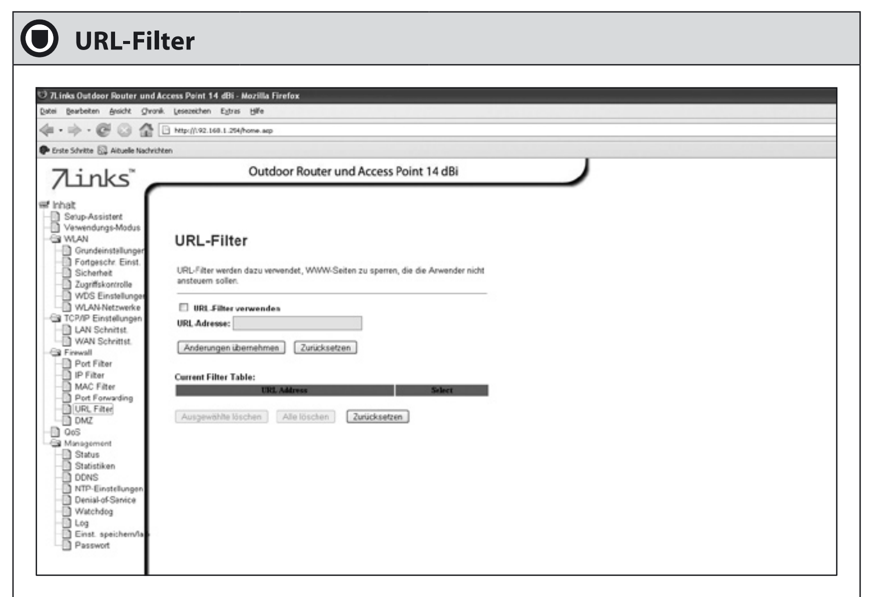
Portforwarding über den Router







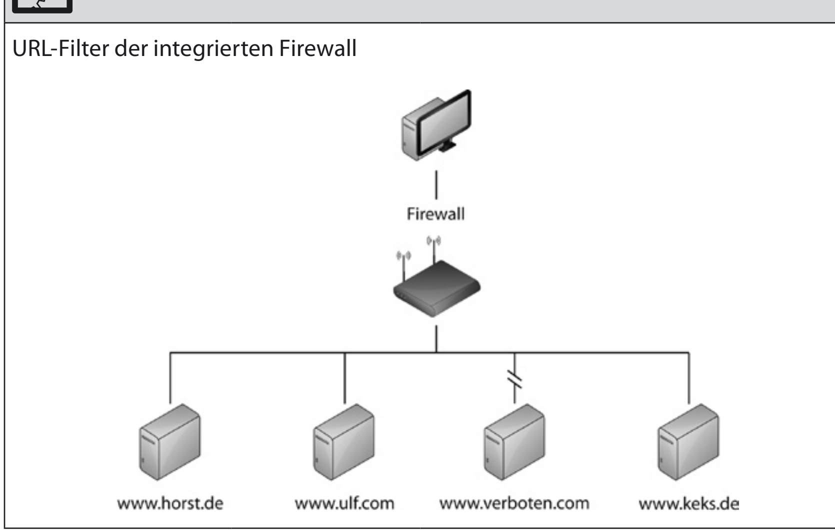

## URL-Filter



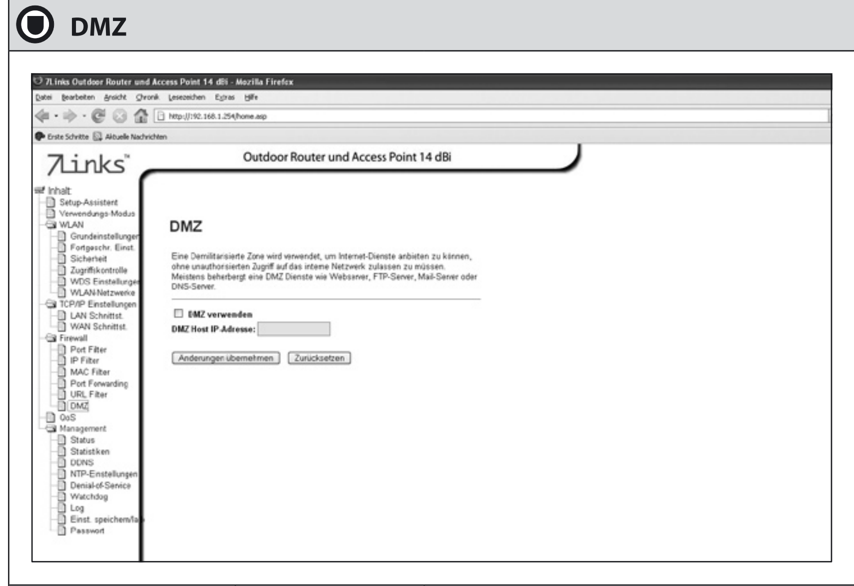

| Option | Werte | Funktion |
|---|---|---|
| **URL-Filter verwenden** | Ein<br>Aus | Filter aktivieren |
| **URL-Adresse** | <text> | Diese URL sperren |

BEISPIELE

URL-Filter der integrierten Firewall



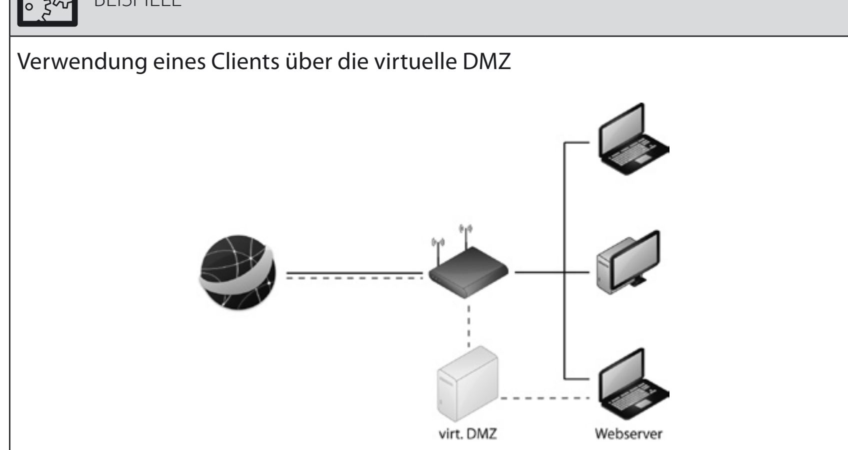
## DMZ




| Option | Werte | Funktion |
|---|---|---|
| **DMZ verwenden** | Ein<br>Aus | Virtuelle DMZ konfigurieren |
| **DMZ Host IP-Adresse** | <text> | IP-Adresse des zu verwendenden virtuellen DMZ-Servers |

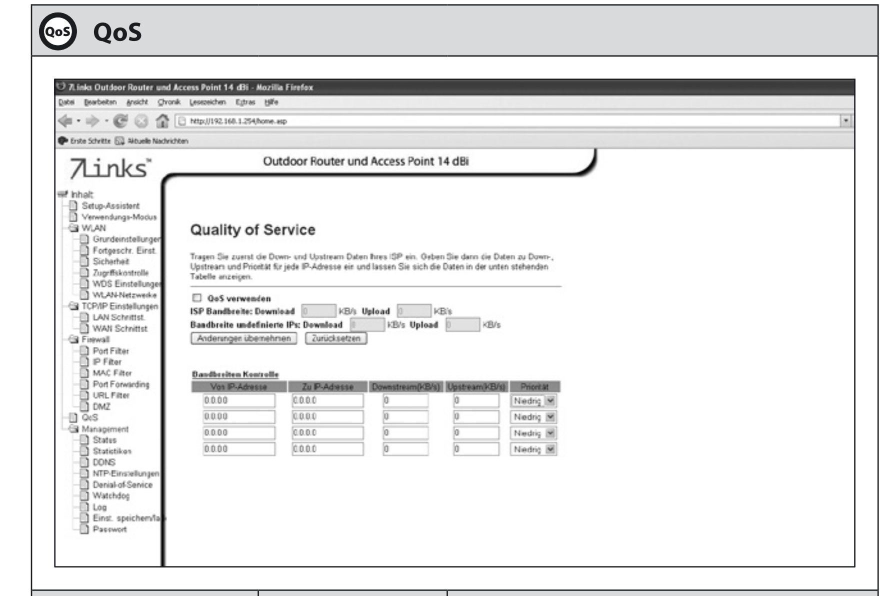
BEISPIELE

Verwendung eines Clients über die virtuelle DMZ



# QOS (QUALITY OF SERVICE)

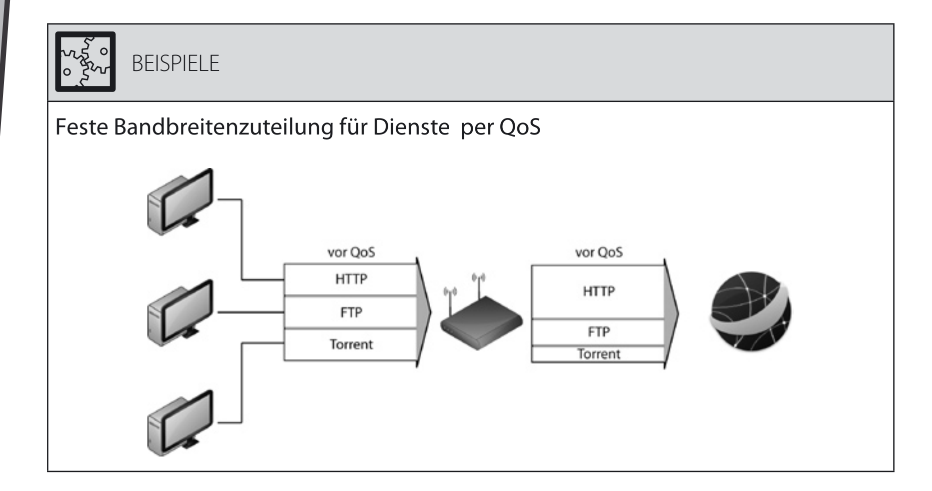
## QoS




| Option | Werte | Funktion |
|---|---|---|
| **QoS verwenden** | Ein<br>Aus | Bandbreitenzuteilung aktivieren |
| **ISP Bandbreite Download** | <text> | Maximale Downloadbandbreite des ISP |
| **ISP Bandbreite Upload** | <text> | Maximale Uploadbandbreite des ISP |
| **Bandbreite undefinierte IPs - Download** | <text> | Maximale Downloadbandbreite für nicht priorisierte Clients |
| **Bandbreite undefinierte IPs - Upload** | <text> | Maximale Uploadbandbreite für nicht priorisierte Clients |
| **Bandbreiten Kontrolle** | <parameter> | Verteilung bestimmter Bandbreiten für definierte Clients mit Prioritätskategorisierung |

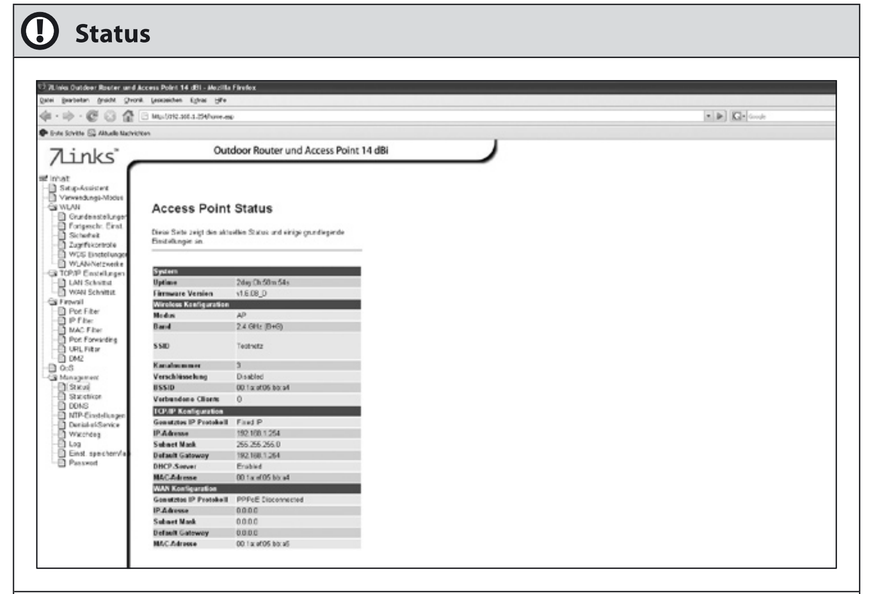
BEISPIELE

Feste Bandbreitenzuteilung für Dienste  per QoS



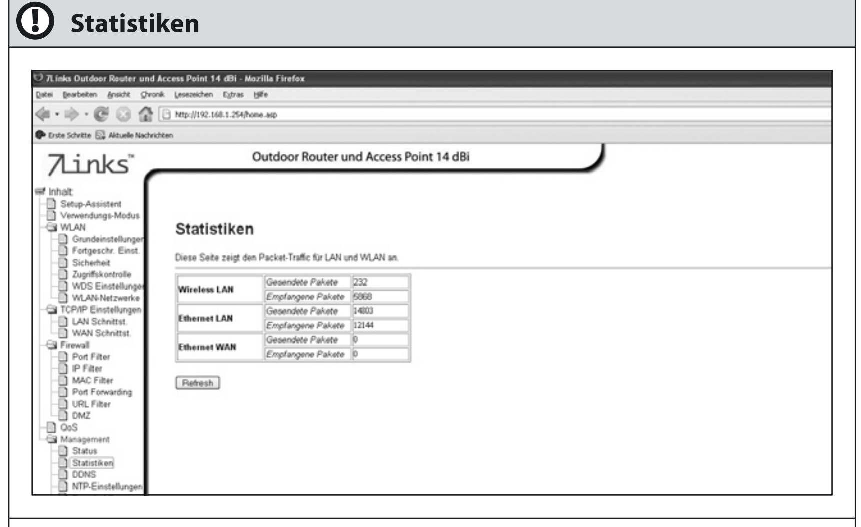
# MANAGEMENT

## Status



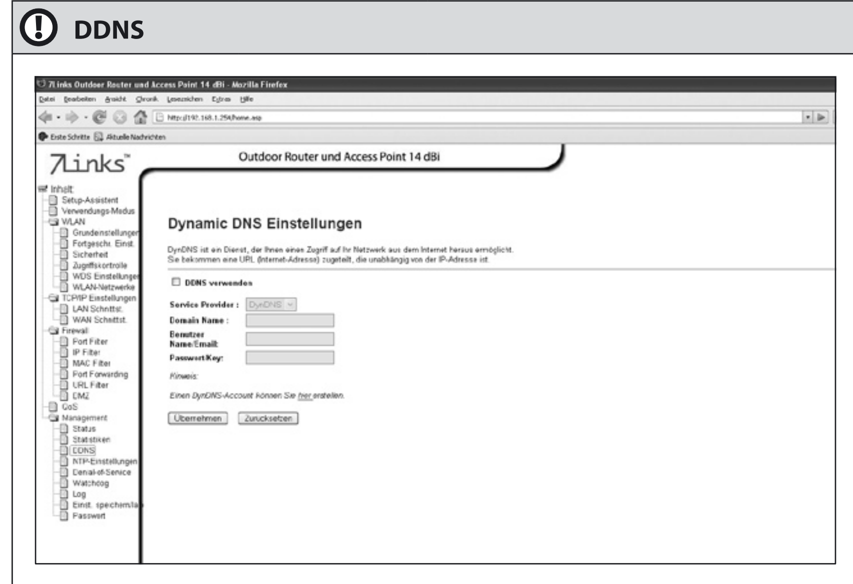

Statusübersicht über alle genutzten Verbindungen

## Statistiken




Statistikübersicht über den Traffic aller genutzten Verbindungen

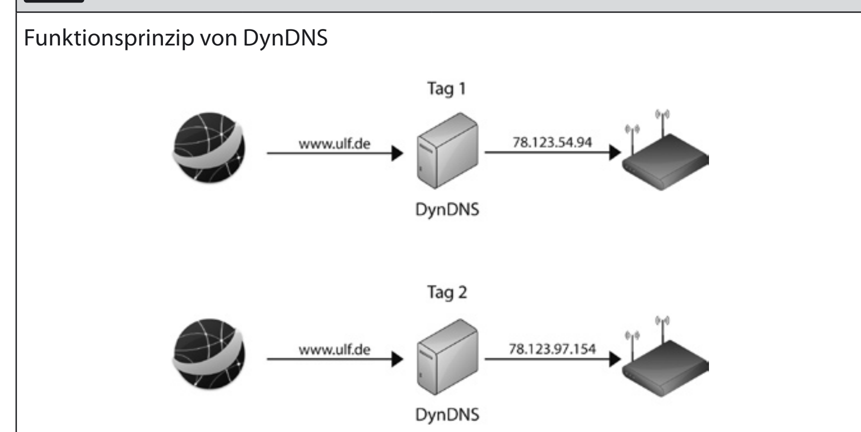
## DDNS




| Option | Werte | Funktion |
|---|---|---|
| **DDNS verwenden** | Ein<br>Aus | Dynamisches DNS verwenden |
| **Service Provider** | DynDNS | Derzeit steht hier nur DynDNS zur Auswahl |
| **Domain Name** | <text> | Zu verwendende Domainbezeichnung |
| **Benutzer Name/ Email** | <text> | Benutzerkennung bei DynDNS |
| **Passwort/Key** | <text> | Benutzerpasswort bei DynDNS |

BEISPIELE

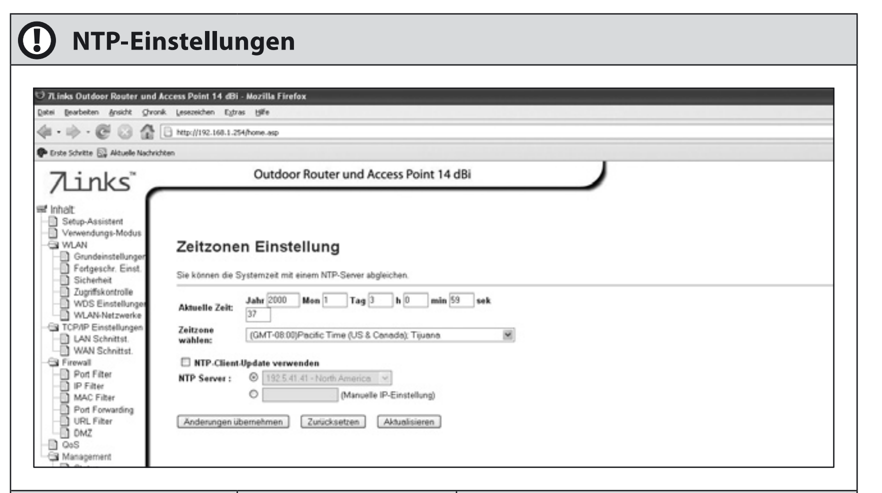
Funktionsprinzip von DynDNS



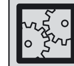




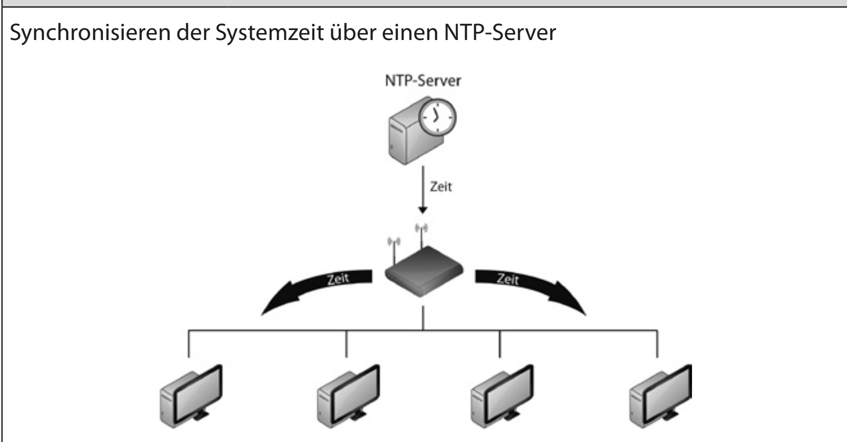

## NTP-Einstellungen




| Option | Werte | Funktion |
|---|---|---|
| **Aktuelle Zeit** | <parameter> | Zeit für den Router einstellen |
| **Zeitzone wählen** | <parameter> | Die Zeitzone einstellen in der der Router steht |
| **NTP-Client-Update verwenden** | Ein<br>Aus | Zeitsynchronisation für Clients aktivieren |
| **NTP Server** | North America 1-3<br>Europa 1-2<br>Australia<br>Asia Pacific<br>Manuell | Externe Zeitserver zur Synchronisation |


BEISPIELE

Synchronisieren der Systemzeit über einen NTP-Server



## Denial-of-Service (DoS)

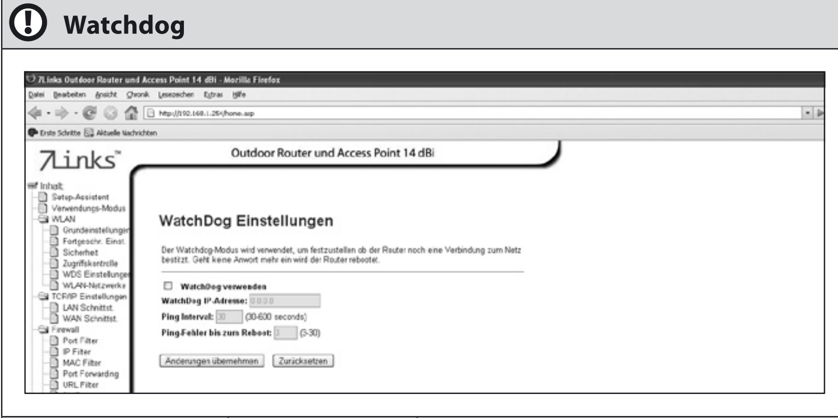
| Option | Werte | Funktion |
|---|---|---|
| **DoS-Schutz verwenden** | Ein<br>Aus | Aktivieren des DoS-Schutzes |
| **Whole System Flood** | Ein<br>Aus<br><text> | Flood Protection, die auf alle externen Anfragen reagiert (DDoS) |
| **Per-Source IP Flood** | Ein<br>Aus<br><text> | Flood Protection, die auf Anfragen von einer Source IP reagiert |
| **TCP/UDP Port Scan** | Niedrig<br>Hoch | **Niedrig** reagiert auf schnelle Portscans, **Hoch** auf zeitlich versetzte Portscans |
| **ICMP Smurf** | Ein<br>Aus | Bei einer Smurf-Attacke sendet ein Angreifer Pings (ICMP-Echo-Requests) an die Broadcast-Adresse eines Netzwerks. Als Absender wird in diese IP-Pakete die Adresse des Opfers eingetragen. Der Router leitet die Anfrage in das innere Netz weiter. Das hat zur Folge, dass alle angeschlossenen Clients dem Opfer auf die vermeintliche Anfrage antworten und damit den Router blockieren |
| **IP Land** | Ein<br>Aus | Verhindert das rekursive Senden von Anfragen |
| **IP Spoof** | Ein<br>Aus | Verhindert die Verschleierung der IP-Adresse eines Angreifers |





| | | |
|---|---|---|
| **IP TearDrop** | Ein<br>Aus | Der Teardrop-Angriff erzeugt eine Reihe Fragmenten. Werden diese Fragmente beim Zielcomputer zusammengefügt, kann er abstürzen oder neu starten |
| **PingOfDeath** | Ein<br>Aus | Als Ping of Death bezeichnet man eine spezielle Attacke, mit dem Ziel, das angegriffene System zum Absturz zu bringen. |
| **TCP Scan** | Ein<br>Aus | Verhindert Scan-Attacken |
| **TCP SynWithData** | Ein<br>Aus | Seltene DoS Attacke, die eine Schwäche mit SynWithData Anfragen ausnutzt |
| **UDP Bomb** | Ein<br>Aus | Verhindert den Absturz des Routers durch ein UDP-Paket, das aus illegalen Werten in bestimmten Feldern aufgebaut ist |
| **UDP EchoChargen** | Ein<br>Aus | Verhindert das rekursive senden/ empfangen von Echo und Chargen Paketen |
| **Source IP Blocking aktivieren** | Ein<br>Aus<br><text> | Detektierte IPs werden für die eingetragene Zeit geblockt |

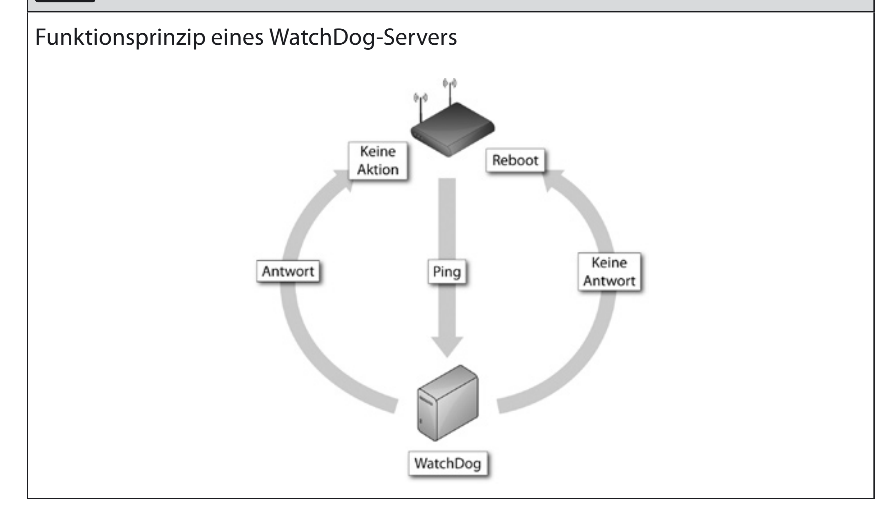
## Watchdog




| Option | Werte | Funktion |
|---|---|---|
| **WatchDog verwenden** | Ein<br>Aus | Watchdog-Server verwenden |
| **WatchDog IP-Adresse** | <text> | IP-Adresse des Clients/Servers, der regelmäßig angepingt wird |
| **Ping Intervall** | <text> | Zeitraum zwischen den Pings auf den Watchdog-Server |
| **Ping-Fehler bis zum Reboot** | <text> | Einstellen wie oft Pings nicht erfolgreich sein müssen, bis sich der Router selbst rebootet |

BEISPIELE

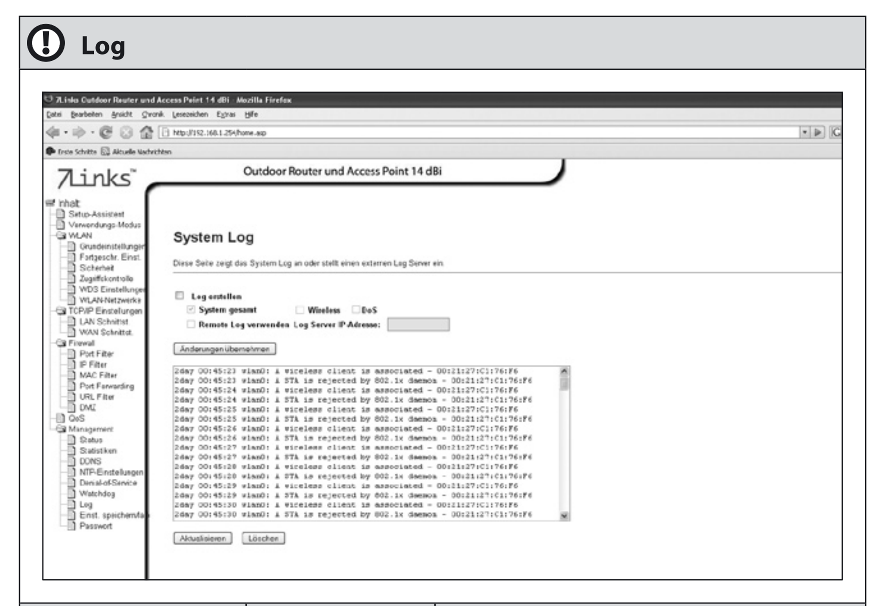
Funktionsprinzip eines WatchDog-Servers








## Log




| Option | Werte | Funktion |
|---|---|---|
| **Log erstellen** | Ein<br>Aus | Betriebslog für den Router erstellen |
| **System gesamt** | Ein<br>Aus | Alle Operationen des Routers aufzeichnen |
| **Wireless** | Ein<br>Aus | Die Wireless-Verbindungen aufzeichnen |
| **DoS** | Ein<br>Aus | DoS-Attacken aufzeichnen |
| **Remote Log verwenden** | Ein<br>Aus | Logs auf einer externen Quelle ablegen |
| **Log Server IP-Adresse** | <text> | IP-Adresse der externen Quelle |

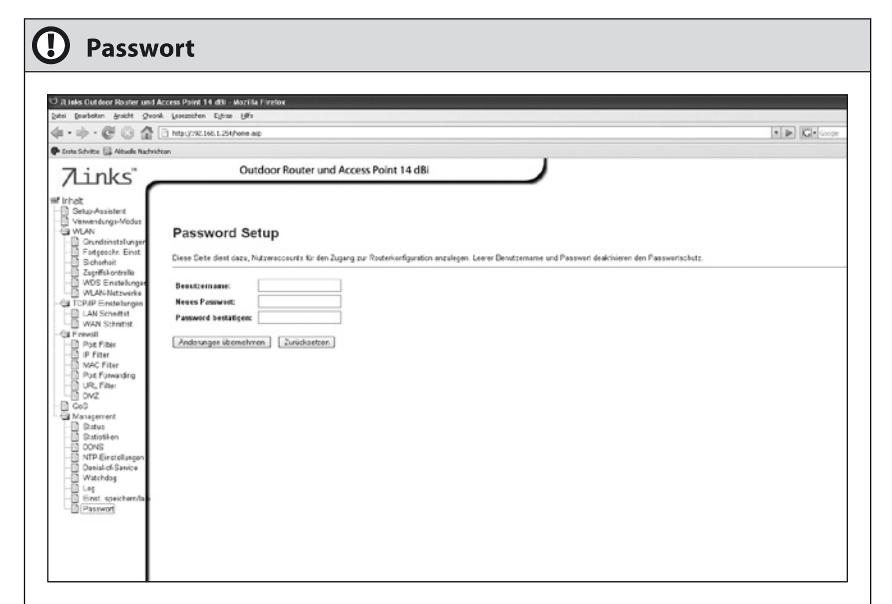
## Einst. Speichern/laden

| Option | Werte | Funktion |
|---|---|---|
| **Einstellungen in Datei speichern** | <datei> | Speichert die Routereinstellungen in einer lokalen Datei |
| **Einstellungen aus Datei laden** | <datei> | Lädt Routereinstellungen aus einer lokalen Datei |
| **Werkseinstel-lungen wieder herstellen** | | Router in den Auslieferungszustand zurücksetzen |





## Passwort




| Option | Werte | Funktion |
|---|---|---|
| **Benutzername** | <text> | Benutzerkennung für Konfigurationsadm inistratoren |
| **Passwort** | <text> | Verwenden Sie unbedingt sichere Passwörter |
| **Passwort bestätigen** | <text> | Passwort nochmals wiederholen |

# ANHANG

# GLOSSAR / BASISWISSEN NETZWERKE

Da bei Netzwerken häufig Unklarheiten und missverständliche Begriffe auftreten, soll dieses Glossar dabei helfen, Licht ins Dunkel mancher Fachbegriffe zu bringen. Im Folgenden werden die grundlegenden Hardwarekomponenten eines herkömmlichen Heimnetzwerks ebenso dargestellt, als auch die verwendeten Anwendungen und Dienste.

**Hardware**

- **Access-Point**
  Der Zugangspunkt oder auch Access-Point ist die „Basisstation" in einem drahtlosen Netzwerk (WLAN). Diese Funktion wird häufig in Heimnetzwerken auch von einem Router ↘ übernommen.

- **DSL-Modem**
  Das DSL-Modem verbindet Ihren Computer mit dem Internet. Wenn Sie mit mehr als einen Computer über eine Leitung Zugriff auf das Internet haben wollen, benötigen Sie einen Router ↘, der direkt hinter das DSL-Modem geschaltet wird.

- **Kabelmodem**
  Als Kabelmodem bezeichnet man das Gerät, das Daten über Fernseh-Kabelnetze überträgt und für Breitband-Internetzugänge über Kabel-anschlüsse (Kabelinternet) eingesetzt wird.

- **Netzwerkhub**
  Netzwerkhubs wurden in der Vergangenheit als „Knotenpunkt" verwendet, um mehrere Netzwerkgeräte miteinander zu verbinden. Jedoch wurden Sie inzwischen weitestgehend durch Netzwerkswitches ↘ abgelöst.

- **Netzwerkkabel/Ethernetkabel**
  Hier gibt es zwei Varianten. So genannte „Patch"-Kabel und „Crossover"-Kabel.
  Patchkabel sind die Kabel, die am häufigsten Verwendung in Netzwerken finden. Sie werden eingesetzt, um Computer mit Switches ↘, Hubs ↘ oder Routern ↘ zu verbinden.
  Crossover-Kabel werden dazu eingesetzt, um zwei Computer direkt miteinander zu verbinden, ohne ein Netzwerk zu verwenden.
  Patchkabel sind der gängige Lieferumfang von Netzwerkprodukten.





- **Netzwerkkarten**
  Netzwerkkarten werden in der heutigen Zeit oftmals schon auf den Hauptplatinen (Mainboards) integriert. Die Anschlüsse ähneln denen von Telefonanschlüssen. Der Stecker hierzu hat die technische Bezeichnung RJ-45. Sie dienen zur Datenübertragung an ein Netzwerk.

- **Netzwerkswitch**
  Switches werden als „Knotenpunkt" von Netzwerken eingesetzt. Sie dienen dazu, mehrere Netzwerkgeräte „auf ein Kabel" im Netzwerk zusammenzuführen. Switches sind häufig zu logischen Verbünden zusammengestellt und verbinden z.B. alle Computer aus einem Büro. Koppelt man mehrere Switches, erhält man ein komplexeres Netzwerk, welches einer Baumstruktur ähnelt.

- **Router**
  Router dienen zur Zugriffssteuerung von Netzwerkcomputern untereinander und regeln ebenfalls den Zugriff auf das Internet für alle sich im Netzwerk befindlichen Computer. Router werden sowohl rein kabelgebunden, als auch als WLAN-fähige Variante vertrieben. Meist übernehmen handelsübliche Router noch Sonderfunktionen wie z.B. DHCP ↘, QoS ↘, Firewall ↘, NTP ↘,…

- **WLAN-Karten und WLAN-Dongles**
  Zunehmend werden drahtlose Netzwerke eingesetzt, so genannte WLANs. Um eine Verbindung zu einem WLAN herstellen zu können, wird eine spezielle Hardware benötigt. Diese Hardware existiert häufig in Form von WLAN-Karten oder WLAN Dongles (-Sticks). WLAN-Karten werden in Desktop-Computern („normaler" Computer) verwendet, während WLAN-Dongles häufig für den mobilen Einsatz gedacht sind (Notebooks) und werden über USB betrieben.

## Grundlegende Netzwerkbegriffe

- **Adressbereich**
  Ein Adressbereich ist eine festgelegte Gruppe von IP- oder MAC-Adressen ◪ und fasst diese zu einer „Verwaltungseinheit" zusammen.

- **Blacklist**
  Mit einer Blacklist bezeichnet man bei Netzwerken eine Liste von Geräten denen die Verbindung zu einem Gerät (z.B. Router) explizit nicht erlaubt ist. Alle anderen Geräte werden von dem Gerät akzeptiert, das den Zugang über die Blacklist regelt. Im Gegensatz dazu steht die so genannte Whitelist ◪.

- **Browser**
  Browser werden Programme genannt die hauptsächlich zur Darstellung von Webseiten genutzt werden. Die bekanntesten Browser sind der Internet Explorer, Mozilla Firefox, Opera oder Google Chrome.

- **Client**
  Als Client wird jede Anwendung bezeichnet, die Daten eines Serverdienstes in Anspruch nimmt. Eine klassische Client-Server Bindung entsteht in Heimnetzwerken häufig schon bei der Vergabe von IP-Adressen im Netzwerk. Hier fordert der Computer als DHCP-Client ◪ eine gültige IP-Adresse vom DHCP-Server (meist der Router) an und erhält diese vom DHCP-Server zugeteilt.

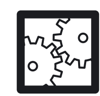
- **Flood Protection**
  Dieser Begriff umschreibt einem Schutzmechanismus von Servern ◪ oder Routern ◪, der diese gegen massive Anhäufungen von Anfragen von außen schützt.
  Der Vergleich eines Damms, der Land gegen Überflutungen schützt gibt dieser Technik Ihre englische Bezeichnung.

- **OSI-Schichtenmodell (Aufbau von Netzwerken)**
  Das OSI-Schichtenmodell dient zur Veranschaulichung der in Netzwerken verwendeten Protokolle ◪. Jede Ebene dieser Modelle baut auf die darunter liegenden Ebenen auf. So ist z.B. einem Gerät eine MAC-Adresse ◪ zugeordnet aber keine IP-Adresse ◪ (bei Switches ◪); jedoch ist einem Gerät mit einer IP-Adresse IMMER auch eine MAC-Adresse zugeordnet.





- **IP-Adresse**
  IP-Adressen werden dazu verwendet Computer, Drucker oder andere Geräte flexibel in ein Netzwerk einzubinden. Hierbei ist zwischen globalen und privaten IP-Adressen zu unterscheiden. Globale IP-Adressen werden von den einzelnen Internet-Anbietern oftmals dynamisch (DHCP ◪) vergeben. Sie dienen dazu, Ihr Heimnetzwerk oder auch nur den einzelnen Computer gegenüber dem Internet erreichbar zu machen. Private IP-Adressen werden im Heimnetzwerk entweder statisch („von Hand" zugewiesen) oder dynamisch (DHCP) vom Anwender selbst vergeben. IP-Adressen ordnen ein spezielles Gerät eindeutig einem bestimmten Netzwerk zu.



BEISPIEL:
IP-Adressen sind die bekanntesten Adressierungen im Netzwerk und treten in folgender Form auf: z.B. 192.168.0.1

- **ISP**
  ISP ist die Abkürzung für „Internet Service Provider". Dieser Begriff wird für Stellen verwendet, die einem Netzwerk oder Einzelcomputer den Zugang zum Internet anbieten. In Deutschland ist der wohl bekannteste ISP T-Online, aber auch Anbieter wie Freenet, Arcor, 1&1 oder KabelDeutschland gehören zu den ISPs.

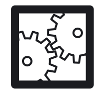
- **LAN**
  LAN (Local Area Network) bezeichnet ein Netzwerk aus Computern und anderen Netzwerkgeräten, die über einen gemeinsamen Adressbereich ◪ verfügen und damit zu einer Struktur zusammengefasst werden.

- **MAC-Adresse**
  Als MAC-Adresse bezeichnet man die physikalische Adresse einer Netzwerkkomponente (z.B. Netzwerkkarte ◪, WLAN-Dongle ◪, Drucker, Switch ◪). MAC-Adressen sind entgegen IP-Adressen ◪ immer eindeutig zuordenbar.
  MAC-Adressen von anderen verbundenen Netzwerkgeräten werden von den einzelnen Geräten jeweils in einer so genannten ARP-Tabelle gespeichert. Diese ARP-Tabellen können zur Fehlersuche dienen, falls ein Gerät ohne IP-Adresse (z.B. Switch) im Netzwerk keine Funktion zeigt.

BEISPIEL:
Eine MAC-Adresse sieht z.B. so aus: 00:00:C0:5A:42:C1

- **Passphrase**
  Mit dem Begriff Passphrase wird ein Schlüsselwort oder Satz umschrieben, der als Sicherheitsabfrage bei der Verbindung zu WPA-/WPA2-Verschlüsselten Netzwerken eingegeben werden muss.

- **Port**
  Als Port wird eine Softwareschnittstelle bezeichnet, die es einzelnen Anwendungen auf Ihrem Computer ermöglicht, mit den Anwendungen eines Anbieters zu kommunizieren. Hier wird hauptsächlich zwischen zwei Protokollen unterschieden: TCP und UDP.



BEISPIEL:
Die häufigste Internet-Anwendung ist ein Browser (Internet Explorer, Mozilla Firefox, usw.), welcher meist über den TCP-Port 80 mit den Servern der Webseiten-Anbieter kommuniziert.

- **POE**
  Power over Ethernet (PoE) bezeichnet ein Verfahren, mit dem netzwerkfähige Geräte über das Ethernet-Kabel mit Strom versorgt werden können.

- **Protokoll**
  Protokolle im Netzwerk sind Standards für Datenpakete, die Netzwerkgeräte untereinander austauschen, um eine eindeutige Kommunikation zu ermöglichen.

- **Pre-Shared Key**
  Mit Pre-Shared Key („vorher vereinbarter Schlüssel“) oder kurz PSK bezeichnet man ein Verschlüsselungsverfahren, bei denen die verwendeten Schlüssel vor der Verbindung beiden Teilnehmern bekannt sein muss (siehe auch WPA/WPA2).

- **Sichere Passwörter**
  Unter sicheren Passwörtern versteht man Passwörter, die bestimmte Bedingungen erfüllen, um von Angreifern nicht mit einfachsten Mitteln entschlüsselt werden zu können.
  Sichere Passwörter sollten generell eine bestimmte Mindestlänge aufweisen und mehrere Sonderzeichen beinhalten. Als Faustregel gilt hier: Je länger das Passwort ist und je mehr Sonderzeichen es beinhaltet, desto sicherer ist es gegen Entschlüsselung.





- **SSID**
  SSID (Service Set Identifier) steht für die Bezeichnung, die für ein WLAN-Netzwerk verwendet wird. Diese SSID wird meist per Broadcast (siehe UDP) öffentlich ausgesendet, um das Netzwerk für mobile Geräte „sichtbar“ zu machen.

- **Subnetz**
  Subnetze sind eine Zusammenfassung von einzelnen IP-Adressen zu Netzwerkstrukturen. So werden meist Computer einer Abteilung im Büro in einem Subnetz zusammengefasst, während die Computer einer anderen Abteilung in einem weiteren Subnetz zusammengefasst sind. Daher sind Subnetze eine reine Strukturierungsmaßnahme. Eine Angabe des Subnetzraumes wird immer in Zusammenhang mit der Vergabe einer IP-Adresse durchgeführt. Im Heimbereich werden normalerweise keine speziellen Subnetze eingerichtet. Daher ist bei Windows-Systemen als Subnetzmaske die 255.255.255.0 voreingestellt. Dadurch stehen die IP-Adressen xxx.xxx.xxx.1 bis xxx.xxx.xxx.254 zur Verfügung.

- **TCP (Transmission Control Protocol)**
  Das TCP-Protokoll wird dazu verwendet, gezielt Informationen von einem speziellen Gegenüber abzufragen (siehe Beispiel bei Port)

- **Traffic**
  Mit Traffic bezeichnet man die ausgetauschten Datenmengen zwischen zwei Stellen oder aber auch den gesamten Datenverkehr in einem Netzwerkabschnitt.

- **UDP (User Datagram Protocol)**
  Das UDP-Protokoll ist ein so genanntes „Broadcast“-Protokoll. Broadcast wird im englischen auch für Radio- oder TV-Sendungen verwendet. Ganz ähnlich arbeitet dieses Protokoll. Es wird verwendet, um Datenpakete an alle im Netzwerk erreichbaren Geräte zu senden und im Weiteren auf Rückmeldung dieser Geräte zu warten. Das UDP-Protokoll wird meist dann von Anwendungen eingesetzt, wenn unsicher ist ob eine entsprechende Gegenstelle im Netzwerk vorhanden ist.

- **uPNP**
  Mit diesem Begriff wird das „universal Plug and Play“-Protokoll bezeichnet. Dieses Protokoll wird hauptsächlich dazu verwendet, Drucker und ähnliche Peripheriegeräte über ein Netzwerk ansteuern zu können.

- **Verschlüsselung**
  Verschlüsselungsmechanismen werden in Netzwerken dazu eingesetzt, Ihre Daten vor fremdem Zugriff abzusichern. Diese Verschlüsselungsmechanismen funktionieren ähnlich wie bei einer EC-Karte. Nur mit dem richtigen Passwort (der richtigen PIN) können die Daten entschlüsselt werden.

- **VPN**
  VPN (Virtual Private Network) steht für eine Schnittstelle in einem Netzwerk, die es ermöglicht, Geräte an ein benachbartes Netz zu binden, ohne dass die Netzwerke miteinander kompatibel sein müssen.

- **WAN**
  WAN (Wide Area Network) bezeichnet ein Netzwerk aus Computern und anderen Netzwerkgeräten, die über größere Entfernungen und aus vielen Bestandteilen zusammengefasst werden. Das bekannteste Beispiel ist das „Internet“. Jedoch kann ein WAN auch nur aus zwei räumlich voneinander getrennten LANs ➘ bestehen.

- **Whitelist**
  Mit einer Whitelist bezeichnet man bei Netzwerken eine Liste von Geräten denen die Verbindung zu einem Gerät (z.B. Router) explizit erlaubt ist. Alle anderen Geräte werden von dem Gerät abgewiesen, das den Zugang über die Whitelist regelt. Im Gegensatz dazu steht die so genannte Blacklist ➘.







**Dienste in Netzwerken**

- **DHCP (Dynamic Host Configuration Protocol)**
  Mit DHCP wird die dynamische Verteilung von IP-Adressen ➘ in Netzwerken bezeichnet. Dynamisch sind diese Adressen deshalb, weil Sie jederzeit ohne größeren Aufwand neu vergeben werden können. Man kann dynamische IP-Adressen auch als geliehene IP-Adressen bezeichnen. Diese geliehenen IP-Adressen werden mit einem „Verfallsdatum“ versehen – der so genannten „Lease Time“. Ein Computer wird am DHCP-Server nur dann nach einer neuen IP-Adresse anfragen, wenn sein „Lease“ abgelaufen ist. Dies ist allerdings auch eine mögliche Fehlerquelle, da es hier zu Unstimmigkeiten zwischen DHCP-Server und DHCP-Clients kommen kann.

*HINWEIS:*
*Windows Computer sind standardmäßig als DHCP-Client eingestellt, um einen einfachen Anschluss an ein Heimnetzwerk zu ermöglichen.*

- **DNS (Domain Name Server)**
  DNS ist ein Serverdienst, der die Übersetzung von IP-Adressen ➘ in gängige Internet-Adressen übernimmt. So wird z.B. aus www.google.de die IP-Adresse: 74.125.39.105. Werden Sie während einer Konfiguration aufgefordert, die DNS-IP-Adresse einzugeben, ist damit immer die Adresse desjenigen Servers ➘ gesucht, welcher den DNS-Serverdienst anbietet. DNS-Server werden aus Gründen der Ausfallsicherheit meist doppelt angegeben und als Primärer DNS (oder DNS1), bzw. Sekundärer DNS (oder DNS2) bezeichnet.

- **Filter**
  Siehe auch Firewall➘

- **Firewall**
  Eine Firewall ist ein Sicherungsmechanismus, welcher meist auf Routern ➘ als Serverdienst läuft, jedoch bereits in Windows (seit XP) integriert ist. Sie erlaubt nur Zugriffe auf voreingestellte Ports ➘, blockt vorher konfigurierte IP-Adressen ➘ und soll generell schädliche Angriffe auf Ihr Netzwerk verhindern.

- **FTP/NAS (File Transfer Protocol/ Network Access Storage)**
  FTP ist ein Serverdienst, der hauptsächlich zum Transfer von Dateien verwendet wird. Dieser Dienst ermöglicht es auf unkomplizierte Art und Weise Dateien von einem Computer auf einen entfernt stehenden anderen Computer ähnlich dem Windows Explorer zu übertragen.

So genannte NAS-Server setzen ebenfalls häufig diesen Dienst ein, um einen Zugriff aus dem gesamten Netzwerk auf eine Festplatte zu erlauben.

- **(Standard-) Gateway**
Als Gateway wird die Schnittstelle bezeichnet, die es den Computern im privaten Netzwerk ermöglicht, mit Computern außerhalb zu kommunizieren. Es ist in diesem Sinne mit Ihrem Router ◪ gleichzusetzen. Das Gateway sammelt und sendet Anfragen der Clients ◪ und leitet diese weiter an die entsprechenden Server ◪ im Internet. Ebenso verteilt das Gateway die Antworten der Server wieder an die Clients, die die Anfrage gestellt hatten.

- **HTTP/Webserver (Hypertext Transfer Protocol)**
Dieser Dienst ist das, was in der Öffentlichkeit als „Das Internet“ bezeichnet wird. Jedoch handelt es sich hier bei nur um eine Vereinfachung, da das Internet an sich eine übergeordnete Struktur ist, welche nahezu alle Serverdienste beinhaltet. HTTP wird zum Transfer und der Darstellung von Webseiten verwendet.

- **Mediastreams**
Diese Gruppe von Serverdiensten wird von vielfältigen Geräten und Anbietern verwendet. Die bekanntesten Beispiele sind Internet-Radiosender, Video-On-Demand und IP-Kameras. Diese Streams nutzen teils unterschiedliche Protokolle ◪ und Protokollversionen. Daher kann es hier durchaus einmal zu Inkompatibilitäten zwischen Server ◪ und Client ◪ kommen.

- **NTP**
NTP (Network Time Protcol) bezeichnet ein Protokoll ◪, mit dem Computer über das Netzwerk Ihre Datums- und Zeiteinstellungen abgleichen können. Dieser Dienst wird von weltweit verteilten Servern bereitgestellt.

- **PPPoE**
PPPoE steht für PPP over Ethernet und bezeichnet Verwendung des Netzwerkprotokolls Point-to-Point Protocol (PPP) über eine Ethernet-Verbindung. PPPoE wird in Deutschland hauptsächlich in Verbindung mit ADSL-Anschlüssen verwendet. ADSL bedeutet Asynchrones DSL und steht für die Verwendung einer Leitung für Telefon und Internet. ADSL ist Standard in Deutschland.
Hauptgrund für die Verwendung von PPPoE ist die Möglichkeit, Authentifizierung und Netzwerkkonfiguration (IP-Adresse ◪, Gateway ◪) auf dem schnelleren Ethernet zur Verfügung zu stellen.

- **PPTP**
Protokoll ◪ zum Aufbau einer VPN ◪-Netzwerkverbindung (Point-to-Point-Transfer-Protokoll).

- **QoS (Quality of Service)**
QoS wird in Netzwerken dazu verwendet, für bestimmte Clients ◪ oder Dienste eine bestimmte, garantierte Bandbreite für den Datenverkehr zu gewährleisten. Als Vergleich lässt sich eine Autobahn heranziehen, auf der selbst bei einem Stau die Standspur von Rettungsfahrzeugen genutzt werden kann, um voranzukommen. QoS wird also immer dann verwendet, wenn sichergestellt werden soll, dass bestimmte Dienste immer verfügbar sein sollen – ohne dabei auf den restlichen Datenverkehr Rücksicht nehmen zu müssen.

- **Samba/SMB**
Mit diesen Begriffen ist ein Serverdienst gemeint, der speziell in Windows Netzwerken verwendet wird. Dieser Service ermöglicht ebenfalls den schnellen und einfachen Zugriff auf Dateien die sich auf anderen Computern befinden (in so genannten „freigegebenen Ordnern“). Jedoch ist dieser Dienst auf Heimnetzwerke begrenzt und kann nur in Ausnahmefällen auch über das Internet in Anspruch genommen werden.

- **Server/Serverdienst**
Ein Server ist immer als Anbieter von Netzwerkdiensten zu sehen. Einzelne Anwendungen werden auch als Serverdienst bezeichnet. Die bekanntesten Serverdienste sind unter anderem Webserver ◪, DHCP ◪ oder E-Mail Server. Mehrere solche Dienste können auf einem Computer oder anderen Geräten (z.B. Routern ◪) gleichzeitig verfügbar sein. Server werden auch Computer genannt, deren ausschließliche Funktion darin besteht, Serverdienste anzubieten und zu verwalten.

- **Statische Adressvergabe**
Bei der statischen Adressvergabe sind alle Netzwerkadressen eines Netzwerkes fest vergeben. Jeder einzelne Client ◪ (Computer) des Netzwerks hat seine feste IP-Adresse ◪, die Subnetzmaske ◪, das Standard-Gateway ◪ und den DNS-Server ◪ fest eingespeichert und muss sich mit diesen Daten beim Server ◪ anmelden. Ein neuer Client (Computer) muss erst mit einer gültigen, noch nicht vergebenen IP-Adresse ◪ und den restlichen Daten ausgestattet werden, bevor er das Netzwerk nutzen kann. Manuelle Adressvergabe ist besonders bei Netzwerkdruckern oder ähnlichen Geräten sinnvoll, auf die häufig zugegriffen werden muss oder in Netzwerken, die besonders sicher sein müssen.

- **Torrents**
  Auch bei Torrents handelt es sich um einen Datei-Transfer-Dienst. Diesen Dienst kann man in gewisser Weise als „verteiltes FTP“ ansehen, da hier der Datentransfer von einzelnen Dateien von mehreren Anbietern („Seeds“) angefordert wird. Dazu müssen die Dateien nicht einmal vollständig beim Anbieter vorhanden sein (diese laden die gleiche Datei ebenfalls herunter – bieten aber schon vorhandene Dateiteile ebenfalls an). Diese „unfertigen“ Quellen werden als „Leeches“ bezeichnet.

- **WEP und WPA**
  Wired Equivalent Privacy (WEP) ist der ehemalige Standard-Verschlüsselungsalgorithmus für WLAN. Er soll sowohl den Zugang zum Netz regeln, als auch die Vertraulichkeit der Daten sicherstellen. Aufgrund verschiedener Schwachstellen wird das Verfahren als unsicher angesehen. Daher sollten WLAN-Installationen die sicherere WPA-Verschlüsselung verwenden.
  Wi-Fi Protected Access (WPA) ist eine modernere Verschlüsselungsmethode für ein WLAN. Sie wurde als Nachfolger von WEP eingeführt und weist nicht deren Schwachstellen auf.







# SICHERHEITSMASSNAHMEN IN WLAN-NETZWERKEN

An erster Stelle sollten der Verzicht von WEP und der Einsatz von WPA oder WPA2 stehen. Dieses Ziel lässt sich in vielen Fällen bereits durch ein Treiber- oder Firmwareupdate erreichen. Lässt sich der Einsatz von WEP nicht vermeiden, sollten folgende grundlegende Behelfsmaßnahmen beachtet werden, um das Risiko von Angriffen fremder Personen auf das WLAN zu minimieren:

- Aktivieren Sie auf alle Fälle den Passwortschutz! Ändern Sie ggf. das Standard-Passwort des Access Points.
- Wenn Sie die WEP-Verschlüsselung verwenden, weil eines der angeschlossenen Geräte WPA oder WPA2 (dringend empfohlen) nicht unterstützt wird, sollte der WEP-Schlüssel mindestens 128 Bit lang sein und eine lose Kombination aus Buchstaben, Ziffern und Sonderzeichen darstellen.
- Aktivieren Sie die Zugriffskontrollliste (ACL = Access Control List), um vom Access Point nur Endgeräte mit bekannter MAC-Adresse zuzulassen. Beachten Sie, dass sich eine MAC-Adresse aber mittels Treiber beliebig einstellen lässt, sodass eine mitgelesene zugelassene MAC-Adresse leicht als eigene ausgegeben werden kann.
- Verwenden Sie eine sinnvolle SSID: Die SSID des Access Point sollte keine Rückschlüsse auf Ihren Namen, verwendete Hardware, Einsatzzweck und Einsatzort zulassen.
- Umstritten ist die Deaktivierung der SSID-Übermittlung (Broadcasting). Sie verhindert das unabsichtliche Einbuchen in das WLAN, jedoch kann die SSID bei deaktiviertem Broadcasting mit einem so genannten Sniffer (Gerät zur LAN-Analyse) mitgelesen werden, wenn sich etwa ein Endgerät beim Access Point anmeldet.
- WLAN-Geräte (wie der Access Point) sollten nicht per WLAN konfiguriert werden, sondern ausschließlich über eine kabelgebundene Verbindung.
- Schalten Sie WLAN-Geräte stets aus, wenn Sie sie nicht benutzen.
- Führen Sie regelmäßige Firmware-Updates vom Access Point durch, um sicherheitsrelevante Aktualisierungen zu erhalten.

Alle diese Sicherheitsmaßnahmen dürfen aber nicht darüber hinwegtäuschen, dass diese letztlich keinen wirklichen Schutz beim Einsatz von WEP bedeuten. Ein erfolgreicher Angriff auf die WEP-Verschlüsselung ist trotz all dieser Vorkehrungen mit den richtigen technischen Voraussetzungen innerhalb von 5 bis 10 Minuten mit ziemlicher Sicherheit erfolgreich.

# INFORMATIONEN ZUR ENTSORGUNG VON ELEKTRISCHEN UND ELEKTRONISCHEN GERÄTEN

Ihr neues Produkt wurde mit größter Sorgfalt entwickelt und aus hochwertigen Komponenten gefertigt. Trotzdem muss das Produkt eines Tages entsorgt werden. Die durchgestrichene Mülltonne bedeutet, dass Ihr Produkt am Ende seiner Lebensdauer getrennt vom Hausmüll entsorgt werden muss. Bitte bringen Sie in Zukunft alle elektrischen oder elektronischen Geräte zu den eingerichteten kommunalen Sammelstellen in Ihrer Gemeinde. Diese nehmen Ihre Geräte entgegen und sorgen für eine ordnungsgemäße und umweltgerechte Verarbeitung. Dadurch verhindern Sie mögliche schädliche Auswirkungen auf Mensch und Umwelt, die sich durch unsachgemäße Handhabung von Produkten am Ende von deren Lebensdauer ergeben können. Genaue Informationen zur nächstgelegenen Sammelstelle erhalten Sie bei Ihrer Gemeinde.







# TECHNISCHE DATEN

| | |
|---|---|
| **Antenne** | 14 dbi Panelantenne |
| **Standard** | IEEE 802.11g/b |
| **Frequenzband** | 2,400GHz bis 2,484GHz |
| **Arbeitstemperatur** | -10°C bis 70°C |
| **Übertragungstyp** | IEEE 802.11g: OFDM(64-QAM, 16-QAM, QPSK, BPSK)<br>IEEE 802.11b: DSSS(CCK/DQPSK/DBPSK) |
| **Datenrate** | 802.11g: 54, 48, 36, 24, 18, 12, 9 & 6 Mbps<br>802.11b: 11, 5.5, 2 and 1 Mbps mit auto-rate fall back |
| **Betriebsluftfeuchtigkeit** | 10% bis 90% (nicht kondensierend) |
| **Zugriffsprotokoll** | CSMA/CA |
| **Anschlüsse** | 1 x Antennenanschluss<br>1x RJ-45 Port für WAN mit POE<br>4 x RJ-45 LAN Ports |
| **Betriebskanäle** | 2.412 bis 2.462GHz (Canada, FCC) / 11 Kanäle<br>2.412 bis 2.484GHz (Japan, TELEC) / 14 Kanäle<br>2.412 bis 2.472GHz (Euro, ETSI) / 13 Kanäle |
| **Stromversorgung** | 12 V/1 A |
| **Sicherheit** | 64/128bit WEP<br>WPA (TKIP mit IEEE 802.1x)<br>WPA2 (AES mit IEEE 802.1x) |
| **Empfindlichkeit** | -68dBm @ 802.11g<br>-80dBm @ 802.11b |
| **Maße** | 253,8 x 231,8 x 87 (LxBxH in mm) |
| **Gewicht** | ca. 800 g |

# CHECKLISTE FÜR DIE KONFIGURATION

| Aufgabe | Erledigt |
|---|---|
| Funkkameraüberwachung ausschalten | |
| Schnurlostelefon ausschalten | |
| Sonstige Geräte mit 2,4 GHz ausschalten | |
| Stromversorgung mit Überspannungsschutz sichern | |
| Firewall am Computer ausstellen | |
| Firewall am vorhandenen Router ausstellen | |
| Virenscanner am Computer ausschalten | |
| MAC-Adressenfilter am vorhandenen Router ausschalten | |
| Verschlüsselung im Netzwerk ausschalten | |
| Benötigte Protokolle notieren | |

| Notwendige Daten | Kommentar |
|---|---|
| Netzwerk SSID | |
| IP – Gateway | |
| IP – DNS-Server | |
| DHCP Range | |
| Subnetzmaske | |
| IP – Internetzugang | |
| IP – Timeserver | |
| Passwort – Internetzugang | |
| Passwort – WLAN | |
| IPs von vorhandenen Servern | |
| IP – Watchdog | |
| IP – Log-Server | |
| IP – virtuelle DMZ | |
| Benötigte Protokolle | |